Session 1B

Security I
Abstract
The Internet today is the main communication infrastructure for private communication and business. A protection against unsolicited traffic such as DDoS attacks is therefore in the interest of all – but, at the same time, security has to be balanced with privacy issues. This paper proposes a collaborative effort against unsolicited traffic where ISPs and end users collaborate. Users define which traffic should be considered as legitimate. ISPs install a network element termed gate to block unsolicited traffic. Moreover, ISPs collaborate by exchanging information among gates to build a global defence against unsolicited traffic. The strength of our solution are that all participants in our solution have incentives to collaborate and participate, and that no changes in the Internet architecture are required.

1. Introduction
The Internet has been designed with the assumption that end systems can be trusted and are willing to cooperate in the Internet. As a result, no security mechanisms have been built into the Internet, and the end-to-end argument has shaped the Internet architecture for several decades. However, the open paradigm where anybody can send any traffic from any source to any destination at any rate at any time has led to incessant Denial of Service attacks, virus and worm spreads with devastating effects. Estimates of malware damage in 2004 run between 169 and 204 billion dollars, or roughly 281 to 340 dollars per Windows computer worldwide, a sharp rise by 100% compared to 2003. Recently, a study by ETH Zurich estimated that a massive Distributed Denial of Service (DDoS) attack on critical Internet elements for one week could produce an economic damage on an entire national economy of CHF 5.83 billion, or 1.2% of the GDP (from: www.mi2g.com).

As easy it is to identify the culprit of the above threat, namely the openness of the Internet architecture and the end-to-end argument, it is as difficult to find an alternative solution to secure the Internet. Reverting the Internet architecture by removing a single “any” of the paradigm may lead to severe threats of privacy or economic imbalances. For example, requesting strict authorization to do away that anybody is allowed to send data opens concerns of privacy. Or, shifting the control of injecting traffic from end systems to e.g. ISPs yields a lot of power to the ISPs to control traffic.

Therefore, we argue that not a confrontation in which either “the network” or “end systems” control traffic, but rather a collaboration between ISPs and users promises to balance the requirements between maintaining the openness of the Internet architecture and ensuring that the security properties are maintained.

This paper proposes an architecture where ISPs and users collaborate to identify, isolate, and mitigate the effects of DDoS attacks and malware spread. In previous work, we have proposed Edge-based Capabilities (EC), an architecture to protect a server or a set of closely located servers against DDoS attacks. EC focuses on protecting a server by inserting a network element termed gate near the server-side edge in the network. The gate is the instance that protects the server from DDoS attacks. This paper leverages the concept of EC to build a global security network where gates exchange information about impending attacks or attacks in progress to protect their networks. Moreover, by sending information upstream towards the origin, an upstream ISP may block attack traffic already before it enters the Internet.

The contributions of this paper are threefold. First, we describe the architectural concepts to build a network of gates and the protocols to exchange information among the gates. Second, we discuss two scenarios on how the architecture can be used against DDoS attacks. Finally, we discuss the incentives to ISPs, service providers, and users to participate, and thereby highlight that the global protection network provides a high level of protection with little deployment effort.

This paper is organized as follows. Section 2 describes the scenario and provides background information on state-of-the-art DDoS attacks. Section 3 describes our architecture where the network and end systems jointly try to defeat unsolicited traffic. After discussing related work in Section 4, we conclude in Section 5.

2. Background
This section provides background information on today’s trends in DDoS attacks and describes our previous work on DDoS prevention called Edge-based capabilities.

2.1. Trends in DDoS Attacks
DDoS attacks come in a plethora of types [1] and constantly evolve to circumvent and defy the countermeasures developed and deployed in the
The drawback of brute-force flooding attacks is obviously that the attacker can easily be identified by the large amount of data it sends towards the target over a long period of time. Over time, we have seen two levels of sophistication in DDoS attacks. First, the increasing "zombification" of end systems allows the attacker to create botnets of over 1 million hosts. Even if just a fraction of bots is used at a given time, large botnet sizes allow the attacker to diversify the attacks in that every zombie can contribute an almost unsuspiciously low attack rate. At the target, however, the aggregation of this traffic is still sufficient to overwhelm the router resources and therefore to deny the service. Such attacks have e.g. been observed on 3G systems where the bottleneck bandwidth of the base station is easily overwhelmed.

Second, the attack patterns have become more sophisticated over time, such as Shrew and RoQ attacks [2,3]. The Shrew attack is a so-called low-rate attack that only sends small high-rate attack bursts, followed by a time of no attack traffic. Therefore, the average attack rate is low. Similarly, Reduction of Quality (RoQ) attacks opt for a reduction in their attack traffic rate to decrease the probability of being detected. Thus, both attacks create a sophisticated attack pattern that is hard to detect and therefore hard to defend against by means of malicious flow detection systems and intrusion detection systems.

2.2. Edge-based Capabilities

In previous work, we have developed a solution to identify and isolate unsolicited traffic in the Internet termed Edge-based Capabilities (EC) [4,5]. EC addresses the key problem in network flooding attacks that the network, and only the network, is able to defy the attack. I.e. the server that notices the attack has no means to directly counter the attack. On the other hand, the network has no means to distinguish unsolicited traffic. A router in the network only sees packets and has no means to distinguish whether the packets were sent from a legitimate user or a malicious sender.

Thus, the concept of EC is that end systems and the network must collaborate in their defence by combining end-to-end authentication with network-based defence, as depicted in Figure 2. First, EC relies on the concept of capabilities [6]. A capability is defined as a permission to send and must be acquired by a sender from a receiver prior to sending data. One possible implementation of a capability are Captchas [7]. Captchas are visual puzzles designed to be easily solvable by humans but difficult for zombies with algorithms such as pattern matching. Thus, when a legitimate user is able to solve a puzzle, it receives an implicit capability that grants access to the server resources. While Captchas are e.g. used to defend against application-layer attacks [8], they cannot directly be applied to protect against network-level flooding attacks.

EC allows a server to hand out capabilities by means of a challenge. A challenge is an abstract term that may be implemented by Captchas. The user that successfully solves the challenge obtains a key. This key allows him to generate cryptographic tags for inclusion in every packet belonging to this flow that is sent to the server. As a result, traffic that can be considered as legitimate in the Internet will carry a valid tag whereas potentially unsolicited traffic does not carry it.

To defend against unsolicited traffic, EC proposes an enforcement element, the gate. The gate is a network element that is deployed by an ISP with the purpose of filtering out unsolicited traffic. By means of the tags, the gate can easily identify and isolate unsolicited traffic.

In our work, we have defined the protocols to ensure a secure and efficient exchange of information among the gate, servers, and clients. In particular, we have selected the gate as the root of a key hierarchy, as the gate as enforcement element is the most trusted entity in this setting. The next level of derived keys is comprised of server-specific keys which are given to the servers that request the protection service the gate offers. The third level are keys specific to both a server and a client. These keys are derived from the respective server key. The advantage of this hierarchy of derived keys is twofold: First, key separation is good crypto hygiene and results in increased security against key compromise. Second, it provides good performance and
scalability, as the gate can derive the keys as they are needed without severe storage overhead.

One key advantage of EC are the incentives. In particular, we argue that each participating party in EC – the ISP, the server and the client, have incentives to participate. First, ISPs that deploy a gate are able to offer an enhanced protection service to the associated servers. Second, associated servers have the incentive to participate because they maintain their reachability even in times of a DDoS attack. If the server uses the keys and forces clients to take the challenge, it remains accessible even during an attack because the requests pass the gate. Finally, clients have the incentive to accept the challenge because their traffic reaches the server. If the edge router is loaded or even under attack, packets of legitimate clients pass the gate with higher priority.

Finally, we have shown that the processing overhead of EC is small, significantly smaller than that of IPsec, for example. Moreover, the overhead can be avoided at normal times when the gate is only turned on when an attack is impending.

3. A Global DDoS Defence Architecture

EC is designed as a solution that can be deployed independently by each ISP. Our main motivation for this independent deployment is the freedom for each ISP to decide if it wants to deploy EC. On the other hand, an independent deployment also has drawbacks. In particular, the protection of EC is limited to a single ISP, the number of scenarios against which EC can provide protection is limited, and the defence itself is limited to the gate itself. In this paper, we therefore argue that EC should be deployed by all ISPs and that the different gates should be interconnected to enhance the protection offered by EC.

3.1. Collaboration among ISPs

The collaboration among ISPs to jointly defend against unsolicited traffic is depicted in Figure 3. The defence requires that multiple gates are deployed within a single ISP and that multiple ISPs deploy gates, ideally all. Gates are still deployed at the edge of the network, not between ISPs, for performance reasons. Depending on the direction into which the traffic flows, gates can be used as egress filters to prevent malicious traffic exiting the network and flooding an access network, as described above, or as ingress filters to prevent that unsolicited traffic even enters the network core.

Thus, we envision two types of collaboration among ISPs in EC. First, a collaboration among gates as egress filters can prevent an attacker from attacking different servers hosted by different ISPs. In particular, given the current size of botnets, it is easy for an attacker to attack multiple targets concurrently or in sequence. Without a coordination among the gates, the attacker can easily refocus its target and the new gate must first learn about the impending attack. Thus, the knowledge that the first attacked gate has is wasted. Instead, with collaborating gates, the knowledge of the first attacked gate is shared among all interested egress gates and therefore allows a gate to build up its guard even before the attack is reaching it. Another advantage is that the information sharing increases the certainty of an attack. If, for some reason, a defence is breached, the information from other gates can be used to counter an attack. Moreover, the information sharing is important for legal purposes. In the attempt of finding attackers and legally proofing that an attack was launched. If a larger number of ISPs can report that a particular attack happened, the evidence is much stronger than if only a single ISP is affected.

The second type of collaboration envisioned is between egress and ingress. In particular, consider that a gate is under attack and it can identify the malicious sender. Then, it can inform the most upstream ISP about the fact that DDoS traffic is spreading from its realm. As a consequence, this upstream ISP is in a position to filter out the malicious traffic already at the ingress. If the attacker spoofs addresses, the egress ISP could inform all ISPs and the one that detects the malicious traffic can block it.

3.2. Protocols for Collaboration

How can ISPs collaborate? We envision two sets of protocols that allow two types of information exchange among the ISPs.

3.2.1. Collaboration During Attacks

A first suite of protocols allows a communication and collaboration at gate-level. Gates thereby directly exchange blacklists of flows or clients that are involved in ongoing or previous DDoS attacks. This information exchange allows the gates to prevent attacks or to react quickly to ongoing attacks. One particular usage of such a direct gate communication can be the reaction against worms or viruses. This type of malware spreads rapidly, and zero-time detection and quarantine is vital to maintain the operation of the Internet. If such an event is detected, information can be spread among gates to block any traffic that is not validly tagged. Thereby, of course, we assume that attackers have not been able to make end systems believe that they are sending legitimate traffic.

However, for efficiency and security reason, we recommend that gates do not communicate directly, but indirectly via a central instance that each ISP defines.
Thus, a gate that is under attack informs the ISP’s central instance. This instance then informs the other gates within its domain as well as the central instances of the other ISPs. This indirection has two advantages. First, it limits the amount of traffic that is exchanged. In particular a gate under attack should not be charged with the task to send out a lot of messages to other gates. Instead, by updating the central instance, communication is limited. Second, the communication among the gates and the central instances as well as among the central instances can be restricted to well-known machines. If any gate can communicate with any other gate, an attacker may try to attack this information exchange by sending wrong information to gates. As a result, legitimate users might suddenly be blocked because gates were misinformed. By defining clear communication paths, the ability to attack the architecture is more difficult. In particular, two ISPs may define that updates must only be exchanged between two predefined hosts. It is obvious that this information exchange needs to be confidential and authenticated. Thus, a cryptographically secured channel must be set up between the communicating central instances of the ISP, e.g. using SSL or IPsec. Preventive Collaboration

A second potential area for collaboration is to carry the information about valid traffic deeper into the network towards its source. However, care must be taken to handle issues of who controls the validation keys and what are the incentives for participating. It makes sense to derive the gate keys for all gates of a single ISP from a single central ISP key, thus extending the per-gate key hierarchy at the roots to form a 4-level hierarchy. However, going one step further to also derive the ISP keys from a global key to allow collaboration would be both a challenge from the security and the incentives point of view. As a solution we suggest that each ISP keeps control over its keys. However, in order to allow identification of legitimate traffic closer to the source the respective remote ISP would need to be entrusted with a local gate or server key. This requires a prior trust relationship between the two ISPs to be established, similar to a peering contract. Then, based on this established trust, the remote ISP closer to the source of the traffic would be given the necessary key of the local gate to validate traffic. For this solution, validity and updates of keys within a single local ISP follow the same structure as the information exchange between gate and server keys. The local ISP defines a single ISP master key, derives gate keys and issues them to the different gates. Note here that since all the considered gates belong to the same ISP, i.e. to the same entity that defines the key, it is possible that all gates receive the same key, as the gates are equally trusted components. However, for security reasons, we advocate for different per-gate keys. For collaboration among ISPs information about valid keys must be securely transmitted to the remote ISP. Here the information exchange occurs only among pre-defined and trusted entities.

We argue that this solution would be feasible for two reasons: First, control over the keys is left with the local ISPs, as the remote ISPs are only the receiving entities, and the local ISP could still run its gate without the help from the remote ISP. Furthermore, the local ISP is still in a position to change the keys, thus staying in control. Second, the solution would scale. Although there are many ISPs in the Internet, this is still a rather limited number compared to the number of flows running through a gate (which is the primary reason for the key hierarchy). Further, each ISP, or transit AS, is clearly identifiable by the global routing tables. Thus, the remote gate can select the right key for tag verification based on the destination address in the packets. At this point, we only sketch this idea because it opens a large design space that can not be addressed in the scope of this paper. But in brief, we have so far considered traffic between end systems, i.e. between a server and client. But traffic in the Internet is not just end-to-end traffic, but contains a plethora of control protocol traffic. This traffic is not protected and secured by EC. If desired, the mechanisms presented by EC could be used to tag control plane traffic. If such an extension that goes beyond the data plane traffic is feasible largely depends on the willingness of ISPs to also share control plane information and the scalability of processing tags also between ISPs, i.e. not at the edge but in the core network.

3.3. Discussion

The extension away from a single gate to a solution where multiple gates of different ISPs collaborate has a number of advantages. First and foremost, a large-scale deployment of collaborating gates at the network edges puts – literally and metaphorically speaking – a fence around the Internet that aims at protecting the network architecture itself as well as benevolently participating Internet users against unsolicited traffic. However, the control of the Internet is not entirely yielded to ISPs, as end systems still define which traffic is legitimate. Learning from the drawbacks of yielding all power to end systems, we argue that the collaborative approach presented in this paper is a synthesis of the strengths of both end systems and the network, i.e. ISPs. By leveraging the concepts of EC to build a global defence allows us to maintain the key advantages of EC, in particular the incentives for all participants. We argue that the benefits in deploying a single gate already provide sufficient motivation for ISPs. The extensions presented in this paper do not require changes in the Internet architecture beyond, and a deployment of a global Internet defence only requires the implementation of the described protocols as well as a central instance for coordination in each ISP. For this slight overhead, an ISP gets in return an enhanced...
protection against ongoing attacks as well as protection against attacks that can not be defied by a single gate.

4. Related Work

EC and the presented extension towards a global defence mechanism for the Internet adds significantly new ideas and concepts to the current state of the art. EC uses authentication schemes to identify and distinguish legitimate from unsolicited traffic. Authentication is a well-known concept, but the unprecedented novelty lies in the joint collaboration between end systems and the network, as well as among ISPs. An alternative approach to authentication is the use of statistical methods to detect misbehaving, unresponsive or suspicious flows. Unfortunately, the traffic patterns of unsolicited traffic are increasingly hard to detect as attacks move away from brute force patterns towards stealthy attacks. Therefore, we argue that authentication schemes provide a more reliable identification.

EC aims at protecting network resources to mitigate DDoS effects. Related work focuses on protecting end system resources [8,9]. Since the resources are complementary, the work is orthogonal and we advocate for integrating the two approaches. Again, end-system defence can be made in isolation, whereas our work emphasizes the collaboration between end systems and networks.

To protect network resources, EC is first a cross-layer solution that requires a collaboration of different layers. In contrast, SOS [10] or Mayday [11] are overlay solutions. They first require modifications to route traffic through the overlay, and second still allow attacks on the underlying infrastructure. Furthermore, SANE [12] is an approach to protect enterprise networks by deploying augmented switches at layer 2. The system works by authorizing routes for the packets between sender and receiver, and needs to deploy a large number of the augmented switches.

Another network-layer protocol is IPsec. The authentication header AH [13] of IPsec can ensure the integrity of the packet. The overhead of IPsec is significant as it authenticates the whole payload. Furthermore, it is stateful, as it needs to store a security association for each pair of communicating machines. EC and the proposed extensions, in contrast, are stateless and therefore provide better scalability, which is vital for a global defence mechanism. The proposed solution emphasizes collaboration among gates as well as among ISPs. Closely related approaches that also target network layer resources, such as SIFF [14] or IP traceback schemes (e.g. [15, 16]), require that all or a large part of the Internet routers be modified and do not provide the same, direct incentives to implement and deploy such an architecture.

5. Conclusion

Security and protection against unsolicited traffic affects all players in the Internet: private users, e-commerce sites and ISPs. This paper argues that in the current Internet only a solution where all these players collaborate is feasible. The global defence architecture described in this paper combines the strength of the players and provides incentives to all of them to actively participate in the defence.

The defence architecture also balances the need to protect against security breaches and the privacy demands of users. In our solution, the end systems maintain the choice to define what traffic is legitimate. However, they yield the power to filter out the traffic to the ISPs. Similarly, the collaboration among ISPs yields benefits for all of them. Our architecture does not require ISPs to provide detailed information about network topology or other information they might be reluctant to reveal. Instead, only information from the gates is exchanged to move the defence against unsolicited traffic from a single local gate to a global defence architecture for the Internet.

References

Bridging CardSpace and Liberty Alliance with SIM authentication

Ivar Jørstad\textsuperscript{a}, Do Van Thuan\textsuperscript{b}, Tore Jønvik\textsuperscript{c} & Do Van Thanh\textsuperscript{d}

\textsuperscript{a}ivar@ubisafe.no – Ubisafe - Gamleveien 252, 2624 Lillehammer – Norway
\textsuperscript{b}t.do@linus.no – Linus – Martin Lingesvei 17, NO-1367 Snarøya – Norway
\textsuperscript{c}tore.jonvik@iu.hio.no - Cort Adelers gt. 30, Oslo – Norway
\textsuperscript{d}thanh-van.do@telenor.com - Telenor R&D – NTNU - Snaroyveien 30 – 1331 Fornebu - Norway

Topics addressed: 4. Service Enablers

Abstract
There are today two major Identity Management solutions, namely the Liberty Alliance and CardSpace from Microsoft. Unfortunately, these solutions are not interoperable. This paper proposes an Identity Management solution that integrates both the Microsoft CardSpace and the Liberty Alliance Identity Management. The idea is to integrate the current SIM authentication used in GSM with both Liberty Alliance and CardSpace such that it can be used for Internet services. Indeed, this is a step further than earlier work that uses SIM authentication for WLAN (Wi-Fi – EAP-SIM). To use the mobile phone as the unified authentication token is a compelling idea due to its popularity and high penetration.

Keywords: Identity management, Strong authentication, SIM authentication

1 Introduction
The number of electronic identities, i.e. user names and passwords that each person has, is increasing everyday and the situation will soon be unmanageable for a regular non-technical user. In many cases, passwords are not strong enough to resist attacks like phishing, pharming, etc. and it is necessary with stronger authentication schemes that are more complicated for the users and more expensive for the service providers. The lack of a satisfactory Identity Management system is the main barrier in the development of e-commerce, m-commerce and e-government applications. The need for an open interoperable Identity Management solution is getting more and more urgent. Unfortunately, there are currently several competing and incompatible solutions. First, the Liberty Alliance \cite{1} came up with a federated network identity solution that offers single sign-on enabling the user to visit several web sites without having to log in again. The other major solution is CardSpace \cite{2} from Microsoft which provides a user-friendly to manage multiple identities. Unfortunately, these solutions are not interoperable.

This paper proposes an Identity Management solution that integrates both the Microsoft CardSpace and the Liberty Alliance Identity Management. The idea is to integrate the current SIM authentication used in GSM with both Liberty Alliance and CardSpace such that it can be used for Internet services. Indeed, this is a step further than earlier work that uses SIM authentication for WLAN (Wi-Fi – EAP-SIM) \cite{3}. The idea of making the mobile phone and its SIM a universal authentication token is compelling, since the mobile phone is so common nowadays, and the GSM network is currently the largest mobile network and is ubiquitous in much of the world.

The paper starts by summarising the state-of-the-art solutions for strong authentication and their limitations. Next, a short introduction of Liberty Alliance and CardSpace is given. An overview of our SIM Strong Authentication Service followed by a scenario showing how our SIM Strong Authentication Service works will be depicted. The value brought to users and service providers will be identified. The business opportunities for the mobile operators are also analysed.

2 Limitations of State-of-the-Art Authentication Solutions

2.1 Passwords
As mentioned earlier, the most common authentication scheme today is based on passwords. It is both weak and not user-friendly due to its plurality. There are many issues with user password management, but from a security point of view, there are three main issues:

- **User-friendliness**: It is always possible to propose systems with high security, but if they are not sufficiently simple and friendly, the user will find a way to bypass them.
- **Phishing** (stealing a user’s password by tricking them into giving their credential away to the wrong party): Keep asking gently for a password from a user, and at some point he will give it away. The most well-known methods for phishing user passwords are either to reproduce an almost identical login page to the one the user is used to, or to pretend to be from customer service and requesting a password for some special operation. The main rule of phishing is “if you can lock a user for a reason” then he will be ready to give you all
the passwords he knows to unlock the situation “current one, old one, one from another site…”

- **Brain limit**: Typical users will only remember from three to five logins/passwords. They will either reuse the same credential all over, creating a potential risk of correlation in between service providers, or will stick the most secure one on a “post-it” somewhere on a very well hidden place such as “under his keyboard.”

To tackle the latter problem and other identity related issues, the Liberty Alliance [1] has promoted the concept of federated network identity that enables users to seamlessly jump from one service provider to another using Single Sign-On, while warranting user privacy, and adequate level of authentication for the requested service and provider independence. However, while Liberty specifies how a service provider requests a given level of authentication, it does not normalize how the CoT authentication authority (i.e. Identity Provider) negotiates credentials with, or on behalf of, the principal. The problem of weak authentication then remains unsolved, leaving room for user password Web phishing and Post-It leaking.

### 2.2 Stronger Authentication Schemes

There exist today several strong authentication alternatives that require the user to present at least two factors, i.e. something that you know (PIN, code or password), combined with something that you have (a smart card or an authentication token), or sometimes something that characterizes you (biometrics). The smart card or authentication token may carry One-Time-Password (OTP) or Public Key Infrastructure (PKI). These solutions bring sufficient protection both to users and service providers but, unfortunately, they all suffer from significant drawbacks:

- **Costly infrastructure**: Strong-authentication solutions require specialized security hardware (such as tokens and smart cards), dedicated software and IT server infrastructure. In addition, there is a cost related to the administration of the keys and certificates.
- **Lack of interoperability**: Strong-authentication solutions are quite often proprietary and do not operate with each other.
- **Poor structure**: They do not provide well-defined interfaces that allow integration with new applications or services.
- **Lack of scalability**: Most current solutions are standalone and it is very difficult to extend them to be a global solution that can be used by every user, everywhere and anytime.
- **Cost of deployment**: Not only do special devices have to be given to each user, but each service provider needs to be customized to support the specific API and handshake protocols specific to the chosen device.
- **Because of the cost of deployment, this solution has been mostly limited to protect access gates to a secure zone (typically a VPN for an enterprise).**

### 2.3 Dynamic Passwords

One alternative addressing some of the mentioned issues is to provide users with dynamic passwords they can use to log in. The users do not have to remember them, and there is no risk of compromised passwords since they are used only once. All users need is a mobile phone that is capable of receiving the password as an SMS message from the service provider. This solution is, however, not very user-friendly since the users have to type in the password. In addition, a system for generating dynamic passwords is also needed and may be costly.

Because of the lack of user friendliness, this solution can not be used for day to day operation, and is mostly limited to exceptional operations such as connecting to the Internet from a hotspot at an airport, hotel, gas station, etc.

### 3 Introduction to Liberty Alliance

The Liberty Alliance [1] uses the concept of network identity which refers to the global set of attributes that are contained in an individual’s various accounts with different service providers. Currently the user’s network identities are like isolated islands and the user is responsible for remembering numerous usernames and passwords for each of these identity islands. The user will typically either try to always use the same password or to record the password somewhere. Either way, the result is a drop in the level of security.

![Figure 1 A Liberty Alliance Circle of Trust](attachment:image.png)
The most logical solution to the problem caused by the isolated network identity is to build bridges that interconnect them together and allow information flows between them. This is precisely what “Federation” is doing. Federation refers to the technologies that make identity and entitlements portable across autonomous policy domains. Consequently, the Federated Network Identity is a portable identity.

The establishment of federated relationships between service providers will hence allow the users to move more seamlessly from one service provider to another one. However, if every service provider has to make alliance to each of the other service providers it will be time consuming and require tremendous efforts. For n service providers, it requires n(n-1)/2 established relationships.

To circumvent this problem, the Liberty Alliance proposed a new role called Identity Provider. The Identity Provider assumes the management of the users Federated Network Identity and the user authentication. A Circle of Trust is group of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.

Figure 1 shows a Circle of Trust. The Principal is the user, employer, customer, game user, etc. whose Federated Network Identity is managed by the Identity Provider. Once federation is done, the user can enjoy Single Sign-On.

4 Introduction to CardSpace

CardSpace [2] is Microsoft’s latest proposal for secure digital identities. CardSpace, originally code-named "InfoCard", lets any Windows application, including Microsoft's own applications such as the next release of Internet Explorer and those created by others, and its users a common way to work with digital identities. Part of the .NET Framework 3.0, CardSpace will be available for Windows Vista, Windows XP, and Windows Server 2003.

Figure 2 CardSpace and interaction among user, relying party and identity provider

CardSpace provides the user with a consistent way to work with multiple digital identities, regardless of the kinds of security tokens they use. The user can create, use, and manage these diverse digital identities in an understandable and effective way. She might also be able to choose from a group of identity providers as the source of the digital identity she presents to the relying parties.

5 Bridging Liberty Alliance and CardSpace

5.1 High level requirements

While the Liberty Alliance alleviates the burden of managing multiple identities by linking them together as a federated identity, CardSpace simplifies the management through a unique interface called Information Card. The identity management concepts used in the Liberty Alliance and CardSpace are completely different. It is hence almost impossible to make them operate together.

Recognising this fact, the requirements imposed on the bridging solution are as follows:

It must be possible for a user to be enrolled in both Liberty Alliance and CardSpace identity management solutions.

It must be possible for the user to use the same authentication scheme, namely SIM authentication in both identity management solutions to reduce the complexity for the users.

The bridging solution called Unified Strong SIM authentication allows the use to use the mobile phone to log into a Liberty Alliance Circle-of Trust and a Microsoft CardSpace environment.

When visiting a Service Provider belonging to the Telenor’s Circle-of-trust the user will be redirected to the Telenor’s Identity Provider for sign in. The user can use his mobile phone to authenticate himself. After successful authentication, the user is logged onto the Service Provider. After a while if the user visits another Service Provider belonging to the Telenor’s Circle of Trust, he does not have to sign in again. Single Sign-on is provided.

Now, if the user visits a web site which does not belong to the Telenor Circle-of-trust but is a Relying Party, i.e. uses the Telenor’s authentication service, he can use the Telenor ID card in CardSpace to do the authentication. Again, the authentication is carried out via his mobile phone.

5.2 Overall architecture

The architecture of the Unified SIM strong authentication is depicted in Figure 3. The heart of the
system is the Telenor’s Identity Provider (IDP). It is communicating with all the entities and supervising all the interactions:

- On the Internet side, it is able to communicate with
  - All the Liberty Alliance Service Providers that has joined the Telenor’s Circle-of-Trust and provides the SIM strong authentication service to them
  - All the CardSpace Relying Parties that uses the Telenor’s Identity Card and offers the SIM strong authentication service to them.

- On the mobile network side, it is able to communicate with
  - The SMS (Short Message Service) gateway to perform authentication using EAP-SIM [4] protocol toward the users’ mobile phones.
  - The AAA (Radius) server [5] [6] that again is communicating with the Telenor’s HLR (Home Location Register) via the MAP gateway to carry out the user’s authentication.

The Telenor’s IDP consists of two main elements:
- A SUN Access Manager which is a Liberty Alliance compliant Identity Provider
- A Microsoft STS (Security Token Service)

Since the Unified SIM Strong Authentication Service is an extension of the SIM Strong Authentication [7], which is offered in a Liberty Alliance Circle-of-Trust with the SUN Access Manager as the main element, an interface has been introduced to bridge with Microsoft’s STS. In addition to management and information exchanges methods, this interface offers an Authentication request method that allows the STS to initiate the entire authentication based on the SIM card.

5.3 Interface between LA IDP and Microsoft STS

To allow the Microsoft STS to use the same authentication mechanism as the LA IDP, a new component has been introduced into the Sun Access Manager at the Telenor IDP site. This component acts as a proxy towards the authentication solution for the Microsoft STS. The Microsoft STS has been configured to perform authentication requests towards this proxy, which in turn initiates authentication with the Strong SIM authentication service.

The request performed towards the STS proxy is an HTTP GET request on the following form:

```
http://<HOSTNAME>/Telenor/RequestMsisdn?msisdn= <MSISDN>
```

Where HOSTNAME is the address of the Telenor IDP and MSISDN is the msisdn of the user to be authenticated.

This request will trigger the proxy to initiate authentication by contacting either the SMS GW or the AAA server, according to which type of authentication is performed. The interface above corresponds to the one used in authentication using SMS.

The response to the above request notifies the STS if the user has accepted the authentication (in the case of SMS authentication with explicit user acceptance), or in the case of authentication towards the HLR, if the EAP-SIM authentication procedure was successful.

5.4 Sequence diagrams

Figure 4 illustrates the process of authentication through the Unified SIM authentication solution using Windows CardSpace, an STS and a relying party. Upon accessing a relying party, Windows CardSpace will be triggered on the user computer. The user will pick the Telenor IDP card, and the STS will be contacted to initiate the authentication. The STS is set up to contact the Telenor IDP when presented with this card, which again communicates towards the SMS GW through the STS Proxy. Upon successful authentication, a success message traverses back from the STS Proxy to the STS, which returns a security token to Windows CardSpace. This token is then presented to the relying party, which verifies the validity and provides the user with access to the requested service.
6 Benefits of the Unified SIM Strong Authentication

6.1 Benefits for End Users
The Unified SIM Strong Authentication Service will deliver value to end users in the following ways:

Simple and better control and management of their identities: The user does not have to manage a multitude of passwords. All the end user needs is an operating mobile phone with SIM card.

Better protection and higher level of security: The Unified SIM Strong Authentication Service provides much better protection than passwords.

Ease of use: The Unified SIM Strong Authentication Service is very simple to use and does not require any particular technical skill. The log in is easy and quite intuitive.

Single Sign-On: After a successful authentication, the user does not have to log in again when visiting other service providers using the Unified SIM Strong Authentication Service. The availability of Single Sign-On access is time limited for security purposes.

Universal applicability: The Unified SIM Strong Authentication Service can be used for any service or application.

Global availability: The Unified SIM Strong Authentication Service can be used anywhere and even when there is no GSM coverage. Indeed, even with a non-operational phone due to lack of coverage, the Unified SIM-based authentication can still be performed via Bluetooth.

6.2 Benefits for Service Providers and Relying Party
The Unified SIM Strong Authentication Service will bring the following benefits to service providers:

Better protection and higher level of security: The Unified SIM strong and mutual authentication service provides higher protection of valuable assets and contributes to extending the availability of their services.

Cost savings: By replacing their current password-based authentication schemes, service providers can save money on operation and maintenance costs due to the simplicity of the application

Lower threshold for deployment: Service providers and Relying Partners do not have to invest large amounts of money to deploy the Unified SIM Strong Authentication Service because the mobile operator manages most of the infrastructure. No great technical expertise is required and the Unified SIM Strong Authentication Service fits very well for larger enterprises and SMEs.

Simpler customer management: Service providers and Relying Parties do not have to take care of the password management since the mobile operators will assume this responsibility.

Reach more customers: The Service Providers and Relying Parties may also reach new customers that are subscribers at the mobile operators.

6.3 Benefits for Mobile Operators
For mobile operators, the Unified SIM Strong Authentication Service will bring the following benefits:

New source of revenue: The Unified SIM Strong Authentication Service constitutes an additional source of revenue for mobile operators which are not based on the sale of air traffic. This source of revenue has large potential since it brings value to end users and service providers.

Reuse of existing infrastructure: Because the Unified SIM authentication solution uses the same SIM and HLR infrastructure used for normal GSM and GPRS services, it allows the reuse of the GSM expertise of the mobile operator.

Improved customer loyalty: The Unified SIM Strong Authentication Service will be a valuable service to end users and will hence contribute to improving customer loyalty and reducing churn.

New business customers: As a compelling service, the Unified SIM Strong Authentication Service will attract new customers for the mobile operator.

Strengthened position: By extending the role and the value of the mobile phone and SIM to the computing world, the Unified SIM Strong Authentication Service will contribute to considerably strengthening the mobile operator’s position in the new converged ICT world.

Easy adaptability for the future: Because the Unified SIM strong authentication is based on easily changeable software elements (Active-X supplicant, IDP Java Authenticator, VitalAAA server and Signalware gateway) it can be easily modified and upgraded to support emerging and future technologies. For example: UMTS USIMs, Smart Card based Certificates, Smart Card-based One-Time-Password (OTP) schemes, etc. Because of the flexibility of the platform described in
this paper, it is quite possible to support multiple authentication schemes over a single authentication infrastructure.

7 Conclusion
Today, service providers have to choose between so many authentication and identity management schemes, and users are left struggling with a variety of digital identities. There are too many duplications and divergences in the digital identity world, and it must end. With the Unified SIM Strong Authentication Service, the mobile phone is indeed the point of convergence of CardSpace and Liberty Alliance identity frameworks. The user is offered the freedom and simplicity of participating and visiting all the web sites no matter whether they are a Liberty Alliance Service Provider or a Microsoft’s Relying Party. In addition, high level of security and convenience is ensured via the usage of the mobile phone as a security token.

A proof-of-concept implementation of the Unified Strong Authentication has been completed by Telenor, Gemalto, Linus, Ubisafe and Oslo University College in collaboration with Sun, Lucent Technologies and Ulticom.

8 References

[6] Radius Extension - rfc2869.txt (Radius Extensions – including EAP), IETF
Flexible and Strong Authentication for Next Generation Services

Martin Meßmer, T-Systems (martin.messmer@t-systems.com)
Ingo Friese, T-Systems (ingo.friese@t-systems.com)
Jörg Heuer, Deutsche Telekom Laboratories (joerg.heuer@telekom.de)

Summary
The All-IP-Network vision of next generation networks (NGN) promises a variety of new service opportunities through the seamless integration of traditional telecommunication services with Internet-based services. Fixed mobile convergence (FMC) based on 3GPP and ETSI-TISPAN standards seems to be turning into a reality. This evolution is interesting in particular for combined fixed and mobile operators such as Deutsche Telekom.

When talking about FMC one of the most obvious and urgent questions is how to authenticate the “fixed” Internet user in such a way that he can also be authorized for the use of mobile services such as mobile voice or services based on the IP multimedia subsystem (IMS) like video conferencing or presence. 3GPP’s answer to that question is the generic bootstrapping architecture (GBA) [1]. The GBA enables the authorization of Internet-based services based on a SIM card authentication of the user. While this approach sounds compelling to the mobile operators most fixed-line operators are more reserved about this idea, since it would force them to build up a SIM card infrastructure that is typically not available at fixed-line operators. Besides that, a customer might not want to upgrade to a SIM card subscription just for a single service.

This paper describes an authentication framework based on 3GPP’s GBA that allows for different kinds of authentications based on service requirements and users’ preferences. After a brief explanation of the motivation for and the goals of this approach we will describe the GBA and its functionality. Thereafter, we will describe the proposed authentication framework.

1 Motivation
Most Telco operators are currently aiming at the migration of their telecommunication infrastructure towards an NGN architecture. Since ETSI-TISPAN adopted the 3GPP standards for the core net, both mobile and fixed-line operators are now “talking the same language” with regard to NGN services. FMC is the big picture behind it. But although the required interfaces are well defined and the client technologies are available in various flavors and form factors, NGNs offering real fixed mobile convergence are still a vision of the future.

We think that the NGN idea is experiencing a typical chicken-and-the-egg problem: Telco operators will not invest too much into NGN and FMC as long as they cannot prove that customers are really interested in NGN services, whereas customers won’t show interest into NGN services as long as those services are not available for trying out. One of the main reasons for that vicious circle is definitely the strong authentication requirements of NGN derived from its UMTS roots: NGN services require SIM card authentication. So, one of NGN’s strongest assets – a strong authenticated and fully controlled operating environment for value added services – is at the same time one of its biggest drawbacks: you need to have a UMTS subscription and a SIM card equipped device to use NGN services.

2 Goals
So, how can Telco operators get around these obstacles? Should they take the NGN service environments like IMS and MBMS as a stand-alone approach and strip away those UMTS roots? Should they lower the authentication requirements and fall back on a simple username/password authentication scheme just to attract more users, especially those that are not yet customers? The answer is a clear yes and no!

![Figure 1: Customer Commitment vs. Service Requirements](image-url)

As we’ve learnt in the past, new products will typically do not incite a lot of people to subscribe to long-term contracts at the very beginning. So, offering new
products with different levels of subscription (e.g. credit card payment, ISP account or SIM card) is typically a good idea to reach more customers.

On the other hand, some really valuable NGN services that leverage the customers mobile context information such as his current location, his phone number, instant messaging contact and availability, will definitely require a GSM or UMTS authentication.

We think, the solution to that dilemma is:

*Let the service provider (not the network) define which level of commitment/authentication is needed/supported for which service and let the customer decide which service he really needs and which level of authentication he is willing to use for that service!*

### 3 Generic Bootstrapping Architecture

In UMTS Release 6 the 3GPP has started to define the GAA (Generic Authentication Architecture) as the framework for the integration of Internet-based services into the NGN world. Within GAA the generic bootstrapping architecture (GBA) defines the functions that are required to authenticate a client to a Web-based service using his UMTS subscription.

#### 3.1 Architecture

Figure 2 gives an overview of how the GBA fits into the 3GPP world in comparison to the IMS environment. It highlights the new functions and interfaces introduced by the GBA.

The Network Application Function (NAF) constitutes the HTTP or HTTPS-based service that requires 3GPP authentication. The NAF may be divided into two parts, the Authentication Proxy (AP) and the Application Server (AS). In that case the AP is responsible solely for the authorization of the client, whereas the AS implements the application-specific functionality and relies on the authorization of the AP. Dividing the NAF into AP and AS is an interesting option in a scenario where the AS is operated by a third party Service Provider.

The Bootstrapping Service Function (BSF) is the authenticator, against which the user equipment (UE) has to do 3GPP authentication, i.e. the Authentication and Key Agreement (AKA) protocol using the IMS Subscriber Identity Module (ISIM) [2]. The Zn-Interface [3] of the BSF enables the NAF to verify whether a UE was correctly authenticated against the BSF.

The ISIM/AKA authentication carried out over the Ub-Interface [4] between the UE and the BSF is transported over HTTP messages. Thus, the UE has to implement a HTTP-based ISIM/AKA authentication.

#### 3.2 Bootstrapping Procedure

When a GBA-enabled UE initially tries to access a GBA-protected service via the NAF or AP, it inserts the string “3gpp-gba” into the User-Agent field within the HTTP header to indicate that it supports GBA authentication (see Figure 3). The NAF will verify that the client request contains an HTTP Authorization header carrying valid NAF session keys derived from an earlier 3GPP authentication. While this cannot be the case with the first request, it does include the indication of GBA support, so the NAF will initiate a HTTP Digest authentication by responding with HTTP 401 Unauthorized message. The response also includes within the WWW-Authenticate header the URL of the BSF to be used.

The UE recognizes from the WWW-Authenticate header that it is requested to supply NAF-specific keys derived from an authentication against the BSF. Since it has not yet authenticated against the BSF it initiates the ISIM/AKA authentication by sending a HTTP Get request to the BSF including – in addition to other parameters - its IMS Private Identity (IMPI) within the Authorization header.

The BSF extracts the IMPI from the request and fetches a set of authentication vectors (AVs) for that identity from the HSS. It selects one of the received AVs and continues the AKA protocol by sending back the user challenge within the WWW-Authenticate header of a HTTP 401 Unauthorized response. The UE checks the correctness of the challenge, calculates the corresponding response parameters by means of the ISIM application and sends them to the BSF within the Authorization header of the second HTTP Get request.

The BSF will now compare the response with the expected values and will eventually derive a session key (KS-NAF) and store it together with the self-generated BSF-Transaction Identifier (B-TID). It will then send back the B-TID and a key lifetime parameter to the UE within the HTTP 200 OK response.
The UE will now also derive the Ks-NAF and respond to the initial MD5 challenge of the NAF by using the B-TID as the username and the Ks-NAF as the password.

When the NAF receives the MD5 response, it will fetch the Ks-NAF that belongs to the given B-TID from the BSF via the Zn interface. It verifies the MD5 response of the UE and finally responds to the initial request of the UE with the requested content. Succeeding requests of the UE will include the MD5 authorization header elements, so that the NAF will identify the UE as authenticated until the key lifetime expires.

3.3 Why using GBA as the basis for flexible and strong authentication for NGN services

We think that the GBA serves as an ideal starting point for a framework for flexible and strong authentication for NGN services for the following reasons:

- **NGN standards-based / FMC support:** GBA is defined by 3GPP/Etsi-TISPAN and therefore fits perfectly into the NGN world. Since it can be deployed over any kind of access network including DSL, the architecture is also acceptable to fixed-line operators.

- **Separation of Authentication and Authorization:** The concept of separating the authentication (BSF) from the authorization (NAF/AP) can also be found in similar architectures like SAML 2.0 [5] / Liberty Alliance ID-FF [6] or MS-CardSpace [7]. It enables very flexible and scalable architectures, since the authorization service does not need to know any authentication details.

- **Improved security through hiding of the user identities:** The user identity (here: the IMPI) is only exchanged between the UE and the authenticating party (BSF), it is not visible to the NAF/AP.

- **Accepted strong and mutual authentication mechanism:** AKA is recognized as a strong and mutual authentication method with high security ratings and can be used with 2G (SIM) or 3G (Universal Subscriber Identity Module/USIM or ISIM) authentication material.

- **Separation of authorization and application functionality:** The concept of the AP enables scenarios where the Telco operator can offer authentication/authorization services to third party service providers (SP) in a way that the authentication complexity is hidden to the SP.

3.4 What’s missing in GBA

While the GBA solves the problem of providing Internet-based services to UMTS customers, it does not answer the question of how to provide Non-UMTS users (e.g. fixed-line customers without SIM card or early adopters) with NGN services as described above. The deficiencies of GBA in respect to the envisioned framework for flexible and strong authentication are:

- **SIM/USIM/ISIM authentication only:** This is definitely in contrast to the goal of flexible and strong authentication as described above.

- **AP/AS interface not suitable for third party services:** In order to operate third party services as AS behind a Telco AP a provisioning interface is required for registering the service with its specific authentication requirements.
4 Enhanced GBA

The goals of the proposed architecture (Figure 4) can be summarized as follows:

- enable per-service definable authentication requirements,
- enable per-user definable authentication preferences,
- enable the negotiation of a set of authentication methods that is both suitable for the service and acceptable for the user.

The architecture is an enhancement of the GBA and therefore we call it ‘Enhanced GBA’ or ‘EGBA’ for simplicity. The enhancements affect the application server (AS), the authentication proxy (AP) and the GBA client, but not the BSF.

The architecture is backward-compatible in the sense that existing GBA clients implementing the standard Ua interface can interoperate with APs that implement the enhanced Ua’ interface and vice versa.

4.1 AP’

AP’, the enhanced AP, plays a key role in the EGBA. As with the GBA AP’ is responsible for the authorization of the UEs to the ASs. The new functions of AP’ are:

- Managing authentication requirements of the application servers
- Negotiating the authentication method(s) to be used by the UE

While in GBA the AP has only one Zn interface to a single BSF, AP’ may have multiple Zn interfaces to various authentication servers.

4.2 AS’

AS’ is an application server that use the AS-REG Interface to register its authentication profile at AP’. An authentication profile is a list of authentication alternatives, each of them consisting of a list of required authentication methods. Each authentication method description includes:

- A unique identifier for the authentication service to be used by the UE
- The URL of authentication server that serves the Zn interface

4.3 Authentication Servers

Authentication servers (e.g. AAA servers or Identity Providers/IdPs) are comparable to the BSF within the GBA. They are responsible for authenticating UEs and are also required for authentication verification through AP’. While the actual authentication mechanism implemented on the interface between the UE and the authentication server can be almost anything and is therefore beyond the scope of this architecture, the interface to AP’ is the Zn interface (Web Services based) as defined within the GBA. Therefore, the authentication method realized by the authentication server has to fulfill the following requirements:

- to derive a temporary user identifier that is delivered to the UE (equals the B-TID)
- to derive a temporary key that can also be derived by the UE (equals the Ks-NAF)

4.4 HTTP-EGBA

As with the GBA the UE is responsible for the authentication and for the interface to the NAF. While in GBA there is exactly one authentication interface, namely the Ub interface to the BSF, in EGBA there may be multiple authentication interfaces depending on the UE’s configuration and the user’s preferences. This leads to the following EGBA specific task on the UE:

- Identification of local available authentication methods
- Management of user’s preferences: which authentication should be used for which AS
- Negotiation of suitable authentication methods for a specific service over the Ua’ interface
- Dispatching of the negotiated authentication methods

The EGBA-specific tasks are bundled in the HTTP-EGBA functional module so that it can be leveraged transparently by any HTTP-based application such as Internet Browsers.

4.5 AS-REG Interface

When an application server starts up, it registers with AP’ by calling a Web Service-based function RegisterService() (see Figure 5).
The registration parameters are the unique AS identifier and the list of authentication alternatives as described in chapter 4.2. AP’ will check the availability of the Zn interface of each of the named authentication methods and if successful, will store the authentication profile for that AS and return a positive response to the AS. AS is now reachable via a unique URL that is derived by AP’ from the unique AS identifier.

4.6 Ua’ Interface

The Ua’ interface is depicted in Figure 6. The initial request of the UE is directed to the AP’-URL that identifies the requested AS. The HTTP-EGBA recognizes from the URL the AS in question and looks up the user’s authentication preferences for that particular AS. Like the GBA procedure HTTP-EGBA will insert an indication for all supported authentication methods into the HTTP header (e.g. “3gpp-gba” for GBA-compliant authentication) and forward the request to AP’. When AP’ receives the request, it identifies the requested AS by the URL, looks up the authentication profile of that AS and checks whether any of the authentication alternatives is supported by the client.

If so, AP’ will respond with a HTTP 401 message including an MD5 challenge and the indication of the first authentication method of that alternative. This triggers the client to initiate the requested authentication and return the MD5 challenge with temporary ID and key derived from the first authentication. AP’ extracts the temporary ID from the MD5 response, fetches the associated temporary key from the authentication server via the Zn interface and checks the validity of the response.

AP’ will then repeatedly challenge the UE for each of the required authentication methods in the authentication alternative in the same way. In the case of all authentication methods being successfully passed, AP’ forwards the request to the named AS.

If AP’ cannot find a suitable authentication alternative for the UE, it will challenge the UE with the first authentication method of the first alternative. This will trigger HTTP/EGBA to give up the authentication and forward the HTTP 401 response unmodified to the application.
5 Status of Work

The EGBA concept is currently being researched in the context of the Deutsche Telekom Laboratories project “Next Generation Network AAA”. At the moment, the proposed framework is at the concept finalization stage. The interface enhancements have not yet been defined down to the protocol elements. For the actual syntax and notation of the authentication requirements the SAML 2.0 concepts of authentication contexts and authentication context classes have been evaluated but not decided on. For the UE side of the EGBA framework Microsoft’s CardSpace technology will be examined.

In parallel with the ongoing conceptual work, a pure GBA testbed has been developed and successfully demonstrated. The testbed is based on OpenIMS [8], which is an open source IMS testbed developed by Fraunhofer Institute FOKUS. The OpenIMS has been complemented by a BSF and NAF implementation from Fraunhofer FOKUS and an HTTP/GBA module and software-based ISIM module of T-Systems Enterprise Services. The HTTP/GBA module is implemented as local HTTP proxy and works on Windows platforms including Windows CE.

6 Conclusions

The proposed EGBA architecture enables the integration of Internet- and NGN-based services. It is intended to offer Telco operators more flexibility regarding the supported authentication methods, thus enabling a broader range of product subscription alternatives for new NGN services and a smoother migration path towards SIM card based authentication. The framework is backward compatible and fully interoperable with latest NGN standards. The newly introduced interface towards the application server enables also wholesale business with third party service providers positioning the Telco operator as the first choice authentication provider for any Internet-based service.

7 References

[2] 3GPP TS 33.102; “Security architecture”; V7.1.0; December 2006
[3] 3GPP TS 29.109; “Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3”; V7.5.0; December 2006
[4] 3GPP TS 24.109; “Bootstrapping Interface (Ub) and Network Application Function Interface (Ua) – Protocol Details”; V7.5.0; December 2006
[6] Liberty Alliance Project; “Liberty ID-FF Architecture Overview”; Version 1.2; (draft-liberty-iddff-arch-overview-1.2-errata-v1.0.pdf)

8 Acronyms

3GPP 3rd Generation Partnership Program
AAA Authentication, Authorization, Accounting
AKA Authentication and Key Agreement
AP Authentication Proxy
AS Application Server
AV Authentication Vector
B-TID Bootstrapping Transaction Identifier
BSF Bootstrapping Server Function
CN Core Net
CSCE Call State Control Function
DSL Digital Subscriber Line
EGBA Enhanced Generic Bootstrapping Architecture
ETSI European Telecommunications Standards Institute
GAA Generic Bootstrapping Architecture
GERAN GSM/EDGE Radio Access Network
GPRS General Packet Radio Service
HSS Home Subscriber System
HTTP(S) Hypertext Transport Protocol (Secure)
IMPI IM (IP Multimedia) Private Identity
IMS IP Multimedia Subsystem
IP-CAN IP Connectivity Access Network
ISIM IM (IP Multimedia) Services Identity Module
ISP Internet Service Provider
MBMS Multimedia Broadcast/Multicast Service
MD5 Message Digest Algorithm 5
NAF Network Application Function
NGN Network Generation Network
SIM Subscriber Identity Module (used in GSM)
SP Service Provider
TISPAN Telecommunications and Internet converged Services and Protocols for Advanced Networking
UE User Equipment
UICC Universal Integrated Circuit Card
UMTS Universal Mobile Telecommunications System
URL Uniform Resource Locator
USIM Universal Subscriber Identity Module
UTRAN Universal Terrestrial Radio Access Network
WLAN Wireless Local Area Network