TrustPass : a trusted passport for mobile users

Exploration Programmes:
Corporate Technology Explores Future Telecommunications

TrustPass: A Trusted Passport for Mobile Users

The development of e-commerce in the business-to-consumer area is partially hindered by the lack of sufficient levels of security, privacy and confidence. The control of the different risks taken by either party is one key factor in the use of e-services. A mobile operator is in a natural and strong position to take a key trusted role. New security technologies which can be used to strengthen the trust relationship between the involved parties are becoming available. At Corporate Technology we have used these new technologies to demonstrate a possible scenario. The potential for a trusted service suited to provide a reliable customer identity ("TrustPass") is shown with a prototype application.

The Exploration Programme "IP Business Support Issues" deals with technologies, services and support functions for IP networks. In detail these are:
- Content oriented IP billing; technologies needed to charge for IP services.
- MPLS Traffic Engineering; how to enable the support of IP-VPN point-to-cloud SLAs with end-to-end QoS guarantees.
- Fraud; what kind of fraud is to be expected when offering services on IP networks and how to prevent such fraud.
- Mobile devices security; which privacy services can be offered for GPRS and UMTS devices accessible from the Internet.
- Security services for the massmarket; easy-to-use security services for Internet users.

With its Exploration Programmes, Corporate Technology is exploring telecommunication technologies and new service possibilities with a long-term view of 2–5 years. Furthermore, the expertise built up in the course of this activity enables active support of business innovation projects.

RENATO CANTINI AND FELIX BAESSLER

Usually, investment costs for a security infrastructure can be justified in the business-to-business area when offering security services. The situation is different in the business-to-consumer area. Nevertheless, opportunities for new service development rise with new security components that are built in the mobile environment.

A number of recurrent issues arises in the business-to-consumer area. Figure 1 shows the relationship between the involved parties and the respective key elements.

A service provider's main concerns are reliable customer information and the fraud risk. The quality of the customer information depends on its source, and the fraud risk on the processes in place and the security mechanisms used.

The customer's main concerns are privacy, the risk of non-fulfilment and the usability aspects. Privacy depends on the control the customer has on the use of own data; the risk of non-fulfilment is somehow reflected by the image of the service provider; in our context, usability depends on how easily a customer can control the use and diffusion of own data.

Part of those issues may either be settled by the legal framework and/or be covered by contracts between the involved parties. Nevertheless, some basic security components must be used to add a sufficient level of trust in the whole picture. Figure 2 shows the interactions and the role of the trusted party, acting as a neutral party that enforces a customer privacy-aware service.

New trust services offer the opportunity to strengthen the customer relationship. With its current position, a mobile operator has a major opportunity to take a trusted party role. If security components are used in an optimal way, the mobile operator can become the guarantor for fair handling of customer privacy while helping to reduce the fraud risk for the service provider.

The mobile operator is in a favourable position due to its strong customer relationship. Smart card technology can be used to offer part of the critical security components needed in the whole picture. The mobile operator already has processes in place that are needed to handle the distribution of SIM cards. By extending the functionality on the network side with additional security components, the mobile operator can take a central trusted party role.

The key factors for the chosen scenario are:
- *Customer data management,* including customer registration and verification. This is a typical key competence in the network access and connectivity service area. It is also related to billing and fraud management issues.
- *Relationship to service providers,* including acquisition of service providers. This is a typical key competence in the portal service area. It is related to the attractiveness offered to service providers, which depends on the addressed customer base and its profile.

The mobile operator can offer a validation service to the service providers. The validation service relies on the following basic components (see overview in figure 3):
- A SIM card with digital signature generation and strong authentication mechanism (known as WIM which stands for WAP Identity Module [1]).

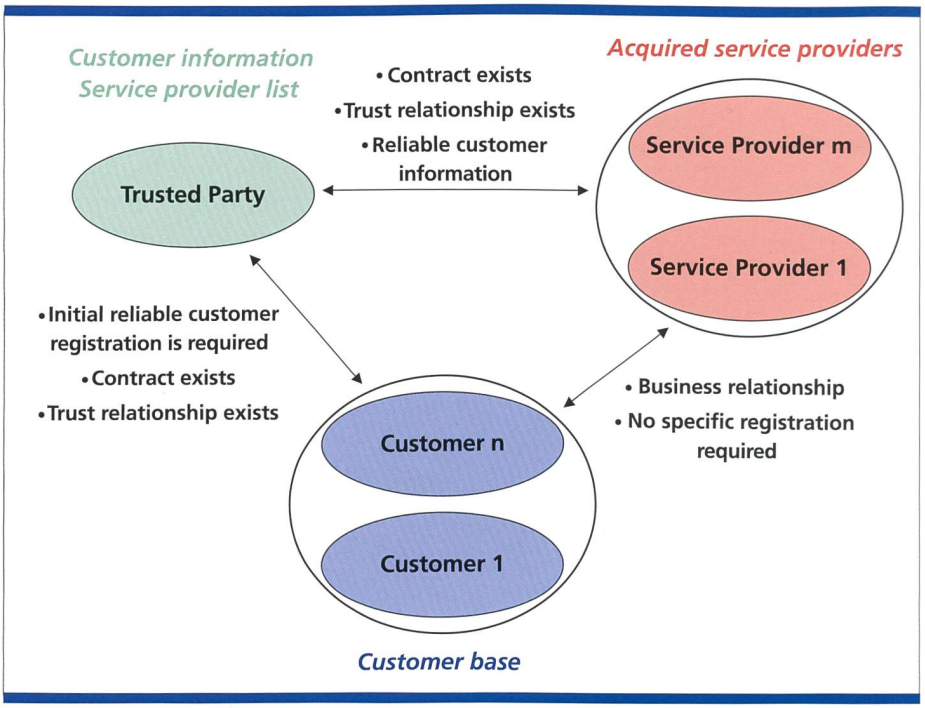

Fig. 1. Relationships and key factors.

– A validation application on the network side.

Relevant Security Standards

The mobile station application execution environment (MExE) defines the security domains and their use. MExE defines a generic model that can be applied to different technologies like WAP and Java.
The wireless application protocol (WAP) is one possible intermediary phase towards the mobile Internet. The WAP standard has defined a new transport protocol and additional application level security. The wireless transport layer security (WTLS) protocol has been optimised for limited bandwidth wireless networks and small mobile equipment with restricted processing power [2]. Digital signature generation on a readable text string is included at the application level (WMLScript). The user is authenticated with a dedicated PIN for each digital signature generation to have a non-repudiation mechanism.

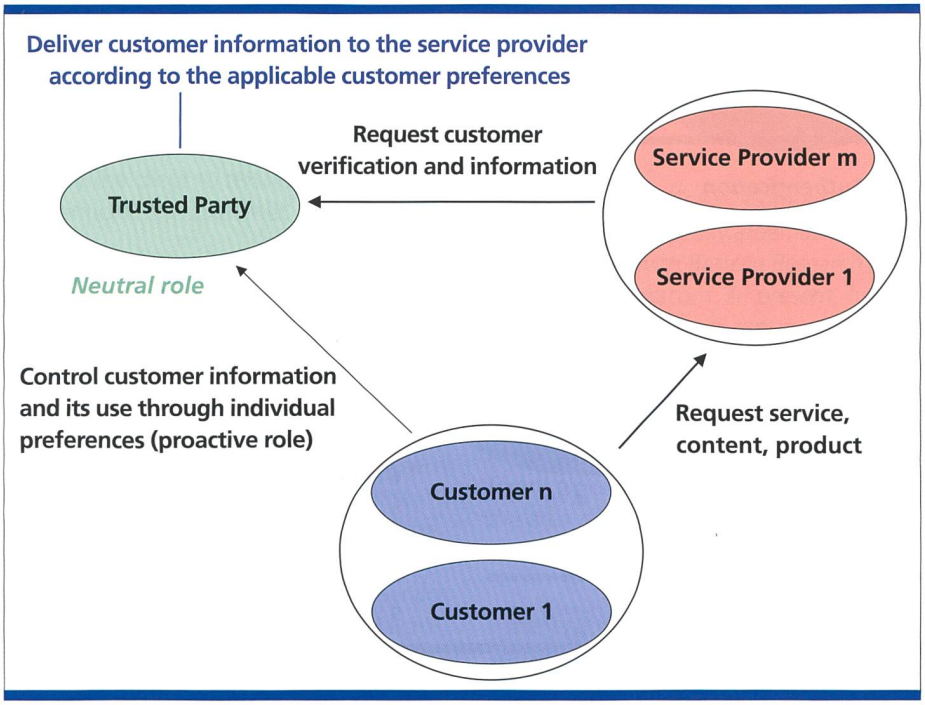

Fig. 2. Scenario for a trusted role.

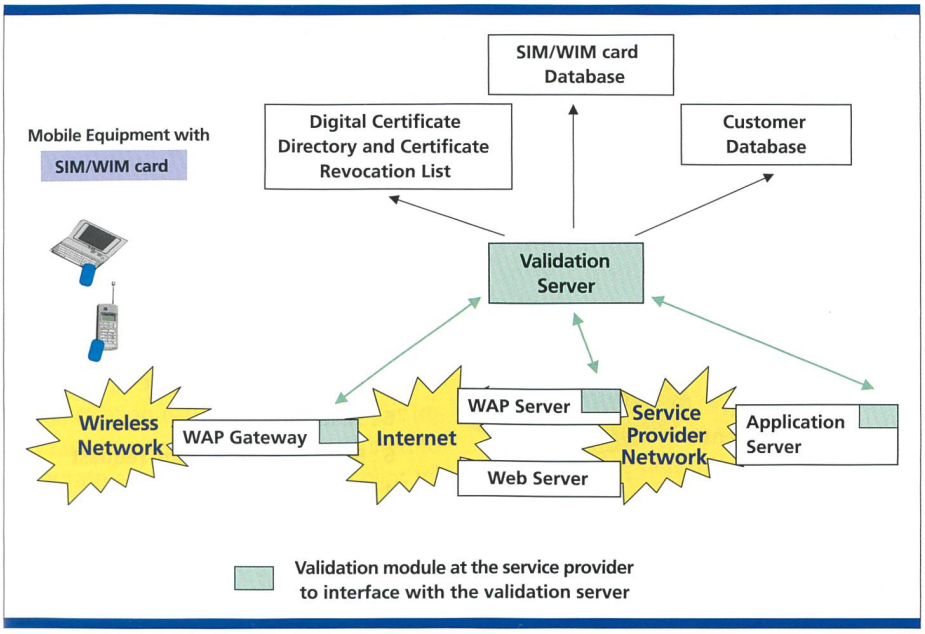

Fig. 3. Overall picture with the required elements.

I-Mode represents an alternative technology which uses the secure sockets layer protocol (SSL, the precursor of TLS [3]), widely deployed in the Internet.
Both WAP as of today (1.x) and I-Mode will converge to WAP-NG (2.x) which gets closely integrated to the Internet. Convergence with the transport layer security (TLS) protocol is included in WAP-NG (version 2.0) [4]. Additional security features at the application level like end-to-end encryption will be added in future WAP-NG versions. Convergence with the XML digital signature (XMLDSig from W3C) is likely to also be added in the future WAP releases.
The wireless Java technology based on Java 2 Microedition (J2ME) does not define security mechanisms on its own but will rather pickup existing ones that are most suited (e.g. from WAP, IETF and 3GPP).

Service Description

A scenario has been defined and implemented at Corporate Technology in the context of the Exploration Programme "IP Business Support Issues" to show one possible trusted party role. The service has been designed with a focus on fair customer privacy handling.
The customer is able to
– access and update own data online,
– select default privacy preferences,
– select service provider specific privacy preferences.

The service provider is able to
– request either customer authentication or digital signature verification,
– request customer information,
– request the explicit customer consent for information gathering.

The trusted party is able to
– register customers that are willing to control the use of own data (out of band process),
– register service providers that want to rely on a central customer information source (out of band process),
– identify and authenticate the service provider,
– authenticate the customer, respectively verify a digital signature generated by the customer,
– send customer information to the service provider on behalf of the customer according to the applicable privacy preferences.

The above mentioned actions use strong security mechanisms and realise integrated processes. As a result, the service of-

fers a reliable and trusted identity that includes a variable level of details.

Design and Implementation

The following tasks were designed and implemented:

- Data model (customer information and preferences, smart card information, service provider information)
- Database administration
- Customer preference handling
- Signed transaction handling
- Demonstration application

Service Requirements

A strong requirement is to rely as much as possible on standard mechanisms on the mobile device side. This reduces the dependency towards the type of mobile devices used. The added value brought by the mobile operator is obtained by a natural combination with existing mobile network infrastructure and an optimum use of the new standard security mechanisms.

From the functional point of view, the customer information needs to be available in the network but does not need to be in the mobile device itself. No data transfer is needed between mobile devices. The functionality is portable between mobile devices as long as the customer uses the same SIM/WIM card. Of course, any mobile device used must support the security mechanisms required for that service. If the customer replaces the SIM/WIM card a new registration process would be required (possibly with optimisations therefore reducing the overheads). The card can be viewed as a key to access customer information. The customer must explicitly accept a type of information to be forwarded by the trusted party to the service provider. The preferences need not to be entered by the customer each time, but may remain valid for a chosen period of time. Hence, customer information may be more or less detailed.

Client-side security is used to enable the scenario that focuses on customer privacy handling by a third trusted party. Customer information is handled according to the service provider's identity and the customer preferences. Remember that the term "privacy" in this context does not mean that no customer information is shared at all, but rather that the customer controls the information sharing and knows which information will be available to a specific service provider. This adds transparency for the customer.

Conclusions

The selected scenario shows a way to strengthen the relationship between the trusted party (e.g. the mobile operator) and the customer by taking a neutral role as a privacy mediator between customer and service provider. The mobile operator can have access to all key elements like the smart card database, the customer database, the digital certificate directory and digital certificate revocation list.

The described scenario may be declined in several variants depending on the preferred SIM/WIM card personalisation process and the targeted customer base. Some options given in the WAP standard are relevant for the described scenario. The preferred variant will depend on the pre-defined business model and the applicable trust relationships.

Depending on the detailed implementation, solutions may be more or less open to external partners.

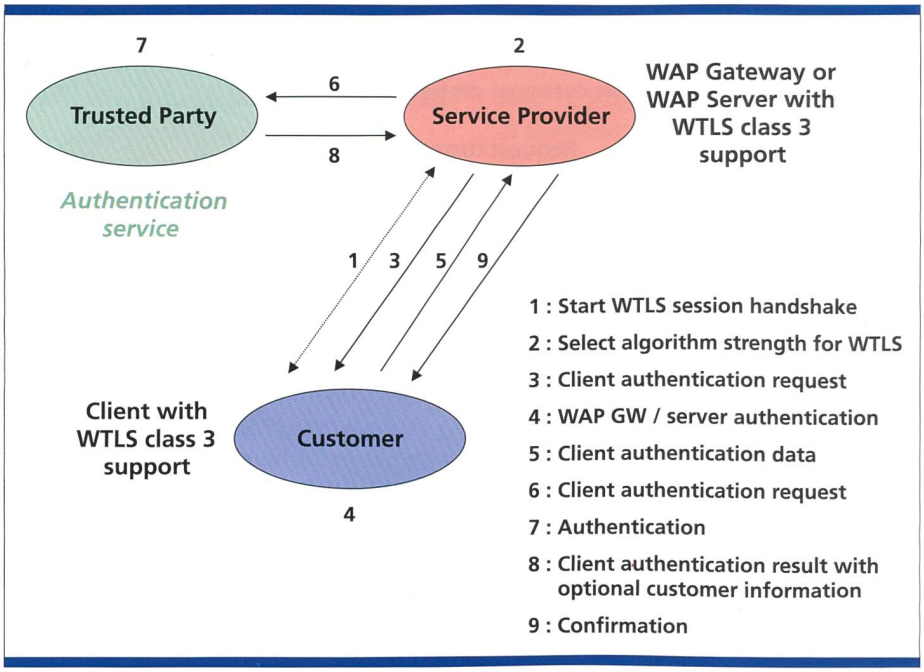

Fig. 4. Validation service for class 3 Wireless Transport Layer Security (WTLS) client authentication.

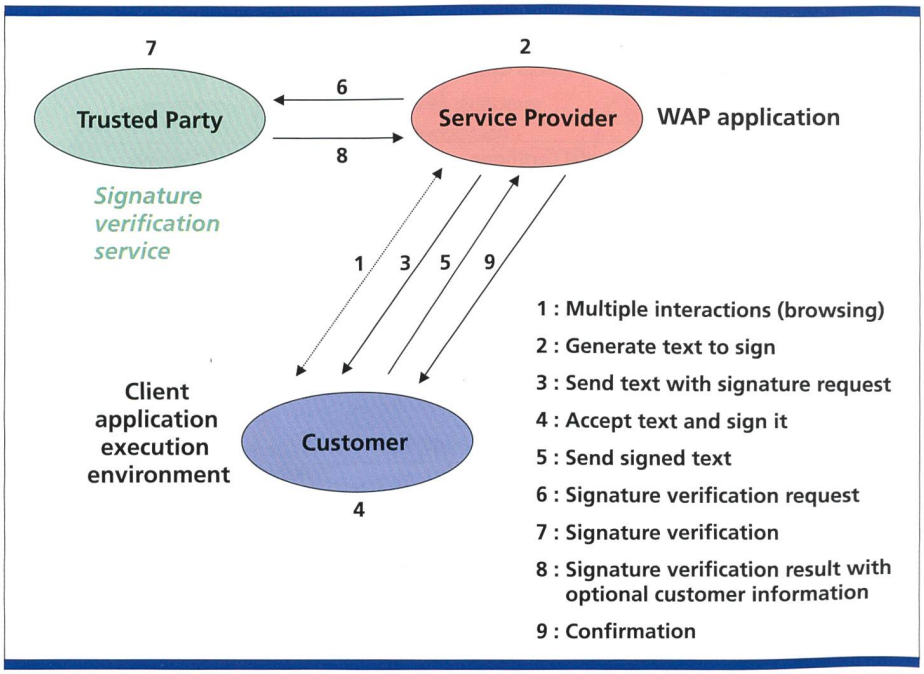

Fig. 5. Verification service for client digital signature.

The service provider needs to install a module to interface with the validation service. This module can be a high level abstraction of the whole validation process that takes place on the trusted party side. The module can be optimised for the described scenario offering a high level application programming interface.
The integration of the validation module in the WAP Gateway or the WAP Server (fig. 4) would require an additional integration effort. A WTLS class 3 compliant implementation includes the client authentication.
The developed trusted-party application focuses on the application layer using WML and WML Script (fig. 5). It verifies the digital signature generated by the customer and uses the signature information sent by the client to securely identify and authenticate the customer.

Comparing TrustPass to Microsoft Passport

The goal of the Passport service from Microsoft is to establish a general-purpose identification service for online customers. This identification service can be used for Microsoft services and for third party services as well. The service providers must integrate the Passport technology on the server side in order to be able to use the Passport service. This identification service is also part of the .NET strategy of Microsoft. The main design requirement has been to offer a way to transport customer information from the Microsoft Passport server to online service providers. The solution works with the common widespread Internet technology.
The proposed TrustPass is targeting a similar service. However, it relies on a different and stronger combination of security components and offers a more versatile privacy handling. Finally, TrustPass outlines a possible alternative architecture that fits well for mobile users

Outlook

The remaining work should concentrate on the integration of both the validation service and the privacy mediation with some existing real applications. This is important to measure the effort required to integrate existing applications. A pilot trial with a pre-selected list of applications and users would be very useful to test the user acceptance.
Due to the evolution of WAP towards XHTML (with WAP-NG), the basic technologies for Internet security like XML digital signature, XML encryption, XML key management system are relevant. The ongoing standardisation work is of primary importance for the e-commerce development. [4]

Renato Cantini *graduated from the HTL Fribourg in 1988 as Dipl. Ing. Electr. and from the EPF Lausanne in 1992 as Dipl. Ing. Telecom. Systems. He worked for 3 years in software development for embedded systems. In May 1995 he joined Swisscom and is working at Swisscom AG, Corporate Technology in the smart card and security field. He leads the MODES project.*

Felix Baessler, *MSc/DIC Computing Science, PhD Applied Mathematics worked for 4 years with Battelle Research before joining Swisscom. At present, he is a member of the security group at Swisscom AG, Corporate Technology, where he is engaged in the development of prototypes of security critical telecom applications. He has acquired expertise in programming different types of smart cards, in particular in the area of Java/SIM technology.*

Pointers

Modes project
http://ctep.swissptt.ch/ep34/projects/projects_modes-en.htm
(Closed User Group)

WAP Forum
www.wapforum.org

Internet Engineering Task Force
www.ietf.org

W3C	www.w3c.org
3GPP	www.3gpp.org
Passport	www.passport.com

Abbreviations

CRL	Certificate Revocation List
J2ME	Java 2 Micro-Edition
SIM	Subscriber Identity Module
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WAP	Wireless Application Protocol
WIM	WAP Identity Module
WML	Wireless Markup Language
WML Script	Wireless Markup Language Script
WTLS	Wireless Transport Layer Security
XML	Extensible Markup Language

References

[1] "Wireless Application Protocol, Identity Module Specification", WAP Forum.
[2] "Wireless Application Protocol, Wireless Transport Layer Security Specification", WAP Forum.
[3] "The TLS Protocol, Version 1.0", RFC2246, IETF.
[4] "WAP TLS Profile and Tunnelling", WAP Forum.

Zusammenfassung

Mit der Einführung neuer sicherer Dienste ergibt sich für Swisscom Mobile die Chance, wichtige Kundenbindungen zu verstärken. Aus seiner angestammten Rolle heraus bietet sich dem Anbieter von mobilen Telekommunikationsdiensten heute die Gelegenheit, die Rolle einer so genannten Trusted Third Party zu übernehmen. Swisscom Mobile bestimmt in diesem Szenario entscheidend die Funktion der Sicherheitsdrehscheibe zwischen Endkunden und E-Commerce-Anbietern.
Alle Beteiligten können von einem solchen Modell profitieren:
- Unseren Kunden garantieren wir nicht nur Sicherheit, sondern darüber hinaus zuverlässige und transparente Privacy.
- Unsere E-Commerce-Anbieter entlasten wir substanziell, indem sie sich nicht mehr um die Details der sicheren Geschäftsabwicklung kümmern müssen.
- Für Swisscom Mobile ergibt sich schliesslich die Möglichkeit, neue Kunden zu gewinnen und gegebenenfalls für kritische Sicherheitsfunktionen Gebühren zu erheben.