



ZebSign ID for Secure eCommerce and mCommerce

Industry

Telecommunications Services
eCommerce and mCommerce

The Company

ZebSign AS, a joint venture of Telenor ASA and Norway Post

Business Challenge

Secure electronic ID suitable for highly secure validation and other security services on several access devices from wire, wireless and other networks

Key Solution Requirements

- Based on enhanced Internet services
- No registration or usage fees for end users
- Ease-of-use, transparent to end user
- Cross-channel utility, suitable for use from several access devices on wire, wireless and other network types
- Supports user validation, single sign-on (SSO), digital signatures, end-to-end encryption and fine-grained authorization using certificate-based digital IDs
- Provide a comprehensive and integrated secure environment for eCommerce and mCommerce businesses

Key Solution Components

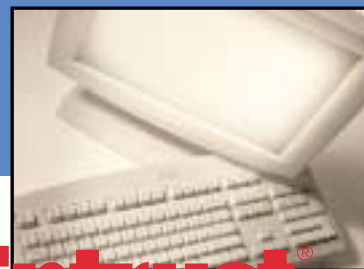
- Entrust Secure Web Portal Solution
- Entrust TruePass™
- Entrust GetAccess™
- Entrust GetAccess™ Mobile Server
- Entrust Authority™ Security Manager
- Entrust Authority™ Roaming Server
- Entrust Authority™ Self-Administration Server
- Entrust Authority™ CMP Toolkit for Java
- SIM Tool Kit 2+ cards for GSM mobile phones and other access devices
- Sun Enterprise Computing Platform with Solaris Operating Environment
- Technical services from Entrust and Protect Data AS

Key Business Results

The relationship between ZebSign and Entrust, provides a comprehensive environment of trust for eCommerce and mCommerce in Norway and the Scandinavian countries, while providing a foundation for further expansion of ZebSign ID services to a larger geographical area.

ZebSign's Strategic Technology Decision

Selection of the Entrust Secure Web Portal Solution to provide stronger security for identification, entitlements, privacy, verification and security management to the ZebSign ID project.



Entrust
Securing Digital Identities
& Information

"The special market conditions in Norway gave us an opportunity to establish a leadership position within security for eCommerce and mCommerce that could later be expanded well beyond our home market. Finding a secure standards-based and flexible solution for user identification and authentication was critical to exploiting that opportunity. It had to be simple and at no cost to the consumer. The solution also needed to provide a single personal ID that could identify a user through any channel (like Internet, Cell phone, Digital TV, etc.) and device that a user might want to utilize across different telecommunications networks. Enhanced Internet security, transparent to the user, is the foundation for the generic 'ZebSign ID' solution.

We needed a framework and infrastructure to create a trusted environment for eCommerce and mCommerce. Originally we planned to develop core technology in-house but then learned that Entrust already had a comprehensive award-winning solution and was continually expanding its range of products and services. The products also covered wireless services where we wanted to concentrate our initial efforts. We evaluated Entrust and based on its excellent technology, its focus on practical implementations in the wireless area and, most importantly, its comprehensive support and technical organizations, we made the decision to team with Entrust. That decision has proved to be an excellent one for ZebSign."

- Dr. Asmund Skomedal
Product Director
ZebSign

"The market conditions in Norway are ideal for the wide-spread use of eCommerce and mCommerce. However, uncertainties about the security in early solutions have kept the users away. New solutions using the ZebSign ID service have been successful, since the ZebSign ID service provides a high level of security, is simple to use and is applicable everywhere. ZebSign is now working closely with its partners to expand the use of electronic ID in their solutions. ZebSign is now launching a security label, to make ZebSign ID the security solution everyone knows and trusts. The ZebSign users will confidently be able to sign up for new Internet and mobile services electronically, as long as the services are based on ZebSign ID, the security solution they can rely on."

Jon Kummen, Managing Director, ZebSign

ZebSign's Background

ZebSign is a joint venture of Telenor ASA, the leading telecom, IT and media company in Norway, and Norway Post. They merged the operations and assets of Telenor ZebSign AS, a business unit within Telenor Mobile Communications, and Ergo Sign AS, a subsidiary of the Ergo Group AB, which in turn is owned by Norway Post.

Prior to the merger, both Telenor ZebSign and ErgoSign were leading players in Norway, developing solutions for secure communication, eCommerce and mCommerce, and providing their partners with electronic identification and electronic signatures. Their new company, ZebSign AS, delivers their services through experienced IT-partners within consultancy, system integration and product development. Solutions for secure communication and eCommerce are supplied to consumers, government agencies, banks and other financial institutions as well as eCommerce and mCommerce businesses.

ZebSign co-operates closely with its owners. With Telenor, ZebSign is able to offer PKI services for many types of telecommunication networks and access devices. With Norway Post, ZebSign uses the national network of post offices for identifying the users, while delivering electronic IDs or shared secrets used for electronic activation. These two owners contribute facilities and skills for the new ZebSign while at the same time, are large customers of ZebSign, assuring them a healthy financial system.

An Ideal Entry Market

There are several circumstances that make Scandinavia, and Norway in particular, an ideal entry market for Electronic ID solutions to support eCommerce and mCommerce.

- Telenor dominates the home market in Norway for all forms of telecommunications and Internet services and is also an active player in the other Scandinavian countries like Denmark, Finland and Sweden.

- Norway Post is an aggressive and innovative player in the development and deployment of security methodologies and technologies for eCommerce and for the physical delivery of merchandise purchased at Web-based businesses.
- The penetration of Internet services is extremely high in the Scandinavian countries and especially so in Norway, where over 50% of households have PC-based Internet access (compared to Germany and the UK, where penetration rates are less than 25%, or to the U.S. with 43% penetration). Telenor is the dominant supplier of ISP services in Norway.
- The usage of mobile telephones and other wireless services is likewise very high in the Scandinavian countries, where over 70 per cent of households have at least one mobile phone-much higher levels of penetration than elsewhere with a rapidly growing range of wireless-based services. Within Telenor-served markets targeted by ZebSign for electronic ID services, the penetration rates are close to 100%.
- Telenor produces more than two million SIM chips each year for use in wireless devices. Over 6 million mobile phones have been sold in Norway, with nearly 3.5 million service subscribers.

¹ **Important footnote:** In this Case Study, the term "electronic signature" is used in accordance with Norwegian government guidelines. Any reference to an "electronic signature" in this study is specifically referring to what Entrust terms as a "digital signature". As outlined in the *Glossary of Key Terms*, a digital signature performs the same functions as a paper signature except that it is fully electronic. It is currently computationally infeasible to forge a digital signature, making it more secure than a paper signature. A digital signature provides the recipient with a means of verifying that the signed content (e.g., data file) came from the person holding the private key that signed the document, and that it has not been altered since it was signed. Digital signatures are becoming increasingly recognized by governments, including the U.S. government, as legally recognized signatures.

"By launching ZebSign, Norway Post and Telenor will offer solutions we believe will improve the foundation for safer commerce and messaging over the Internet. This will simplify eCommerce by tidying up the increasing multitude of passwords and user IDs that today's customers must wade through. This is also in line with the government's aim to establish a 24 hour public administration service that is dependent on secure electronic messaging."

Per Andersen

Managing Director, ErgoGroup, Norway Post
Chairman of the Board of Directors, ZebSign

- Market growth in e-commerce is substantial in Norway. Last year alone has brought 28% growth to this market and more than one third of the population make use of Internet banking and purchasing.

As a result of these market circumstances, eCommerce and mCommerce services have a higher level of acceptance in Scandinavian countries than in most other geographic markets. These and other conditions make Norway an ideal test bed for the development, introduction and evolutionary enhancement of security solutions for eCommerce and mCommerce. These circumstances give ZebSign key market entry advantages:

- Telenor is the dominant telecom (voice), Internet and mobile (wireless) operator in Norway with a substantial customer database and industry expertise.
- Telenor is the voice service provider for all of the large banks and public sector (government) agencies in Norway and is the network services provider for virtually all eCommerce and mCommerce businesses in the country.
- Both Telenor and Ergo group are major players in the development of eCommerce and mCommerce solutions, including outsourcing services.

The ZebSign Business Model

To leverage these favorable conditions, the initial ZebSign business model focuses on two business opportunities:

- ZebSign is positioned as a nationwide certificate service provider (CSP). Providing electronic ID services for communication, to eCommerce and mCommerce businesses across multiple vertical markets, including telecommunications (Telenor's own voice, Internet and wireless customers), financial (banking, insurance and investment), gaming (betting and lottery services), entertainment (including 'infotainment'), retail, transportation, government and healthcare. ZebSign provides a full range of Entrust enhanced Internet security services to product developers, service providers and their respective subscribers.
- ZebSign also offers a packaged solution for both large and small businesses that wish to issue, administer and manage their own

PKI-based solutions for electronic IDs and electronic signatures. This approach has been especially successful with large enterprises, hospitals and government agencies and is moving towards the financial and legal sectors specifically with respect to email and Web access.

The services created to handle these market segments are:

- ZebSign ID is a general electronic ID, similar to a passport or equivalent physical identity card. ZebSign's goal is to provide a single electronic ID solution for all Internet users and service providers in Norway
- ZebSign Pro is an electronic ID service tailored to a customer's need. Customers whose needs are not met by the standardized ZebSign ID, make use of ZebSign Pro. This solution offers the option of customizing the information held in the electronic ID as well as customizing the level of security.

Although initial emphasis for ZebSign is in the Norwegian market, the company's mission and plans call for it to offer electronic ID services on a more widespread basis. ErgoGroup has already started operations abroad and Telenor is an active player in international markets with operations in more than 30 countries. After Telenor's privatization in December 2000, it has increased its international activities in mobile, Internet, satellite and cable TV services. The ZebSign electronic ID solutions match closely with Telenor's global expansion plans and are projected to have special attraction for mCommerce businesses outside as well as inside Scandinavia. The global plans for ZebSign made it especially important to select a

Jon Kummen, Director of Telenor ZebSign had this to say about the selection of Entrust, *"We plan to provide every consumer in Norway with an electronic signature, to meet a strong demand from the banking, finance and retail sectors, as well as from the Norwegian central administration. Central to this is the clear customer requirement to have one 'electronic identity' that can be presented from any combination of devices, like GSM phones, ISDN devices, traditional PCs and laptops, and requiring user registration only once. After considering all leading solutions, we chose Entrust's enhanced Internet security solution as it was the only solution both mature enough to provide a high level of trust, and flexible and scalable enough to let us build one trusted community over all types of networks. Our choice of the Entrust organization as well as its products has more than met our expectations."*

technology partner with global experience and presence. As discussed in the remainder of this report, ZebSign chose Entrust as its enhanced Internet security technology software provider for its digital ID services.

Market Requirements for Electronic ID Solutions

Both Telenor and Norway Post provide a broad range of services to consumers, businesses and public sector agencies (which make up over half the GNP in Scandinavian countries) and are very familiar with market demands and preferences. In defining the market needs for ZebSign ID service they identified several critical criteria for success, these include:

- The ZebSign ID service should not bring any new costs to the end user. There can be no fees for registration, certificate issuance, new devices or added software.
- The ZebSign ID service must offer simplicity in all respects, from registration through log-on through secure usage and sign off from multiple access devices across diverse networks.
- The ZebSign ID service needs simplicity and transparency, to allow Internet users to make use of Internet services based on ZebSign ID without having to install or maintain new equipment or software.
- The ZebSign ID service must support cross channel access. An end user must be able to log on with the same electronic ID from all access devices and networks, with initial focus on PC-based Internet Web access and mobile phone wireless access. Future requirements are expected to include home television, handheld devices such as PDAs, video game devices and public vending machines among others for cable, satellite, wireless and wired networking facilities from low speed to broadband.
- The ZebSign ID service must be offered along with a comprehensive and integrated environment of trust for eCommerce and mCommerce. Functionality requirements therefore include user authentication (CA-based), single sign-on (SSO), fine-grained authorization features, electronically-signed online transactions, electronic signatures on electronic documents for post-transaction records, messaging services and payment services, ranging from micro payments for vending machines to multi-million dollar stock transactions.

- In sum, the ZebSign ID service must offer a highly secure environment of trust readily understood and accepted by end users

To fulfill these requirements, ZebSign had the option to build its own ZebSign ID service with in-house resources and off-the-shelf products from multiple suppliers or to seek a strategic relationship with one or more strategic partners with proven and comprehensive public key solutions. Following a rigorous evaluation of alternatives, Telenor Mobile's ZebSign (prior to the formation of the new ZebSign) chose Entrust as its primary security software provider for the development, integration and deployment of the ZebSign ID service.

The Strategic Relationship between ZebSign and Entrust, Inc.

While still operating as a business unit within Telenor's Mobile Communications group, ZebSign embarked on several initiatives to develop a family of secure electronic identification methodologies in support of eCommerce and mCommerce businesses. Evaluation of alternatives established that Entrust was better able to fulfill the electronic ID requirements defined by ZebSign and Telenor than any other supplier.

In June 2000, Entrust and Telenor entered into an agreement to establish an electronic and mobile commerce communications infrastructure for secured business services to include advanced communications, managed delivery services and content delivery applications via a variety of electronic distribution channels. The enhanced Internet security solution would allow Telenor customers to have secure, easy and no

cost access to eCommerce and mCommerce facilities via the Internet, mobile networks, satellite networks and ISDN. The Entrust and Telenor agreement has been carried over to the new ZebSign organization owned jointly by Telenor and Norway Post.

The Entrust and ZebSign overall relationship also involves support from Protect Data AS, the Norwegian subsidiary of Protect Data AB Group (www.protectdata.com), an international specialist organization operating in the IT security sector. Protect Data AS is an Entrust Value Added Reseller for Norway, and also offers solutions for anti-virus systems, firewalls, user identification systems, virtual private networks (VPNs), secure PCs, content control and other systems for secure eCommerce.

The Key Technology Components of the ZebSign ID Service

The ZebSign ID service is based on current and selected emerging technologies and methodologies that include: public-key infrastructure (PKI); wireless technologies such as "micro" browsers and subscriber identification module (SIM) tool kits, wireless application protocol (WAP) and Universal Mobile Telephone System (UMTS), Java technologies; open UNIX-based computing platform; and Internet portal solutions for single sign on (SSO) and server-centric authentication and authorization.

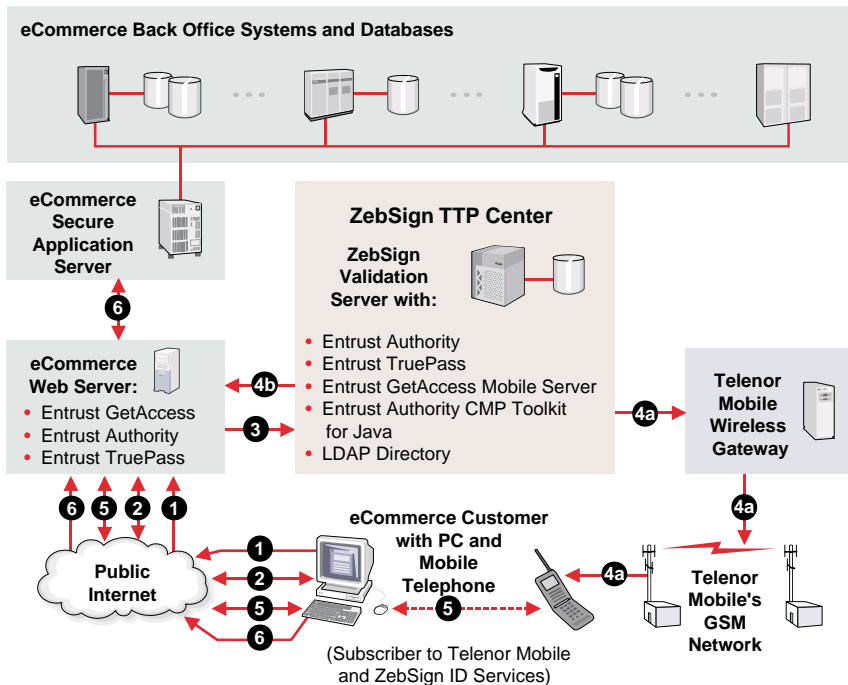
As noted above, many of the technologies and components critical to the ZebSign ID service are licensed from Entrust. These technologies and components are identified below and are followed by a brief identification of other key features found in the ZebSign ID service.

The Strategic Role of Entrust

Entrust is the source for many of the technologies, support services and proven products that are central to the ZebSign ID service. Collectively these allow ZebSign, along with their partners to offer a more secure, trusted environment for their business, government and consumer customers. The Entrust Secure Web Portal Solution delivers enhanced ID, verification, privacy and security management for the ZebSign ID service. Key Entrust products within these solutions include one or more of:

- **Entrust TruePass™** software provides enhanced security capabilities for Web-based applications. These capabilities provide the Entrust Secure Web Portal solution with strong identification, verification, and privacy needed to bring critical business functions to the web. Since Entrust TruePass software does not require client software to be installed or configured on a user's computer, organizations are able to deliver a unique combination of application enablement and roaming access through enhanced security features with unmatched user transparency and ease of deployment. The Entrust TruePass enhanced identification capabilities can also be strengthened by adding incremental requirements for login information, including the ability to use a one-time PIN generated and sent to a mobile phone through an SMS message. This delivers two-factor authentication using the Entrust TruePass capabilities, without the requirement to deploy additional hardware. The capability is available as a packaged service offering through Entrust.
- **Entrust GetAccess™** software is an infrastructure/management solution for secured eCommerce portals serving large numbers of globally distributed customers. It provides the framework within which a comprehensive enhanced Internet security solution can exist and includes single sign-on (SSO), directory services for validation, authorization (entitlement) services and other features and functions. Entrust GetAccess software facilitates personalization with access control management for the variety of data, content and services that are integrated in the Entrust Secure Web Portal. The Entrust GetAccess software integrates with a broad range of applications, including the Entrust TruePass software, which is supported by the ZebSign ID service.
- **Entrust GetAccess™ Mobile Server** extends the selectable authentication, fine-grained authorization, single sign-on (SSO) and personalization capabilities of the Entrust GetAccess software to multiple devices accessed via wireless networks. The combination of Entrust GetAccess software (see above) and the mobile server helps provide the infrastructure necessary for a common secured web portal for both wireless and Web access. It supports an integrated enhanced Internet security environment for enterprise eCommerce and mCommerce across multiple networks to diverse devices.
- **Entrust Authority™ Security Manager** is the public-key infrastructure (PKI) from Entrust that provides user authentication, digital signatures and security to enable the protection of confidential information. Entrust Authority Security Manager delivers the following specific capabilities for enterprise eCommerce and mCommerce solutions: *Certification Authority (CA), Registration Authority (RA), Key and Certificate Management, Key Backup and Recovery, Revocation System, Notarization, User Mobility, PKI Networking, Security Policy Management, Scalability and Interoperability.*

Figure 1: ZebSign Entry Service: Mobile Phone as Out-of-band One-time PIN



Transaction Sequence:

- 1 Customer logs on to eCommerce Web Server from PC via Internet.
- 2 Entrust TruePass prompts customer for Name & Password, which the customer provides.
- 3 Entrust TruePass sends user name to the ZebSign TTP Center.
- 4 The ZebSign TTP Center:
 - 4a ZebSign Validation Server issues a one-time PIN and sends it to the customer's mobile phone (predefined number) via an SMS message
 - 4b Entrust Authority Roaming Server sends the encrypted Entrust TruePass user profile (containing keys, etc.) and the hashed PIN code to the eCommerce Web Server
- 5 Entrust TruePass prompts the customer to provide the PIN, which is done. Entrust TruePass then sends the encrypted user profile to the customer's PC.
- 6 Entrust TruePass decrypts the user profile within the browser, which may then be used online via the Internet for authentication, electronic signature and enhanced encryption. Usually it is used for immediate authentication by the site to allow customer to proceed with a secure online eCommerce transaction.

(Note that this entry service was used prior to the availability of production quantities of SIM 32 KB chips with on-chip encryption co-processor)

- **Entrust Authority™ CMP Toolkit for Java** provides end users with a way to acquire digital (electronic) certificates over the air (OTA) to be used for trusted mobile transactions. It is a component of the Entrust Mobile Solutions family that enables customers to extend their enhanced Internet security solutions to support both wired and wireless users accessing a Web portal via alternative devices. The product is part of one of the world's first mobile commerce payment system enabling the use of digital (electronic) signatures on mobile phones to complete transactions. Mobile commerce applications available today include purchasing theatre tickets, airport transportation vouchers and refreshments from vending machines - with additional mobile commerce applications planned for the future.

- **Entrust Authority™ Roaming Server** allows users to log in and have more secure access to sensitive information from any location without having to carry the digital ID necessary to establish a secured connection. It also provides the flexibility to tailor security roles to match the needs of corporations and end users.
- **Entrust Authority™ Self-Administration Server** allows for easier enrollment, faster deployment, and simpler recovery of digital IDs by providing users with Web-based self-registration and recovery capabilities. In addition, providing users with the capability to self-register can help in reducing overhead costs.

Based on proven products delivered through the Entrust Secure Web Portal solution, Entrust is providing ZebSign with a set of capabilities to help organizations secure the content and data that they make available through their web portal. The Entrust Secure Web Portal solution is unique from other vendors because it provides the security portals required without compromising the flexibility and performance required by customers.

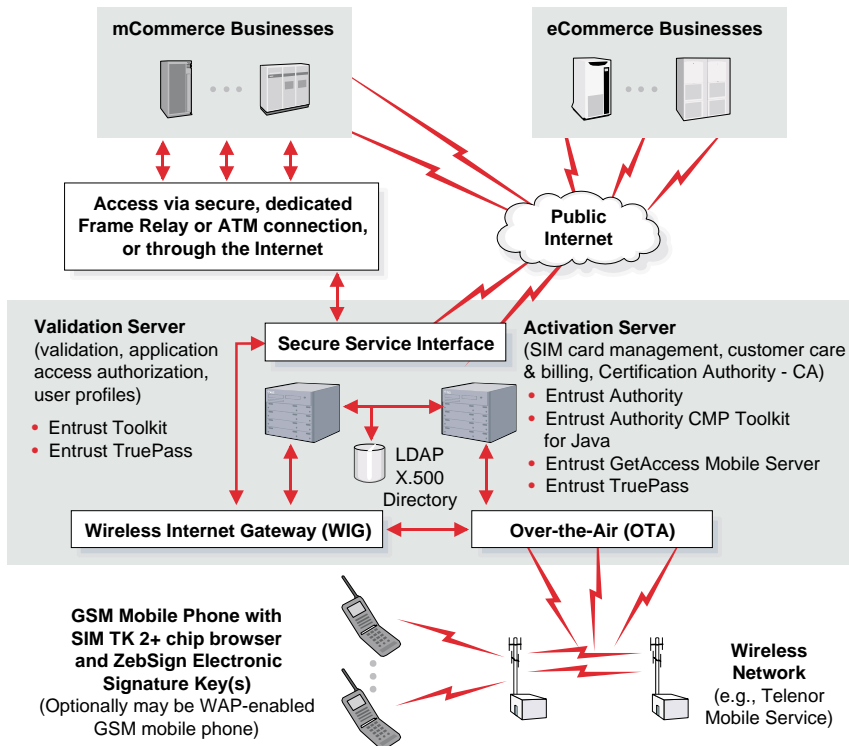
In addition to providing all of the above products, Entrust also provides consulting services and has worked closely with ZebSign in the definition, specification and development of some of its new products as well as with the expansion of features and functions for existing products. Entrust professional services staff members played an important role in assisting ZebSign with design modifications to integrate and deploy the ZebSign ID service, designed to meet the unique needs of its market segments and individual large customers.

Other Technology Components of the ZebSign ID Service

In addition to the critical enhanced Internet security products from Entrust, the ZebSign team has also integrated a number of other key technology components into the ZebSign ID service and associated offers. These include:

- Security products such as firewalls, LDAP

Figure 2: Overview of an Example ZebSign Environment for mCommerce Transactions



directory servers and secure Web or gateway servers from various third-party manufacturers.

- Subscriber Identification Module (SIM) Tool Kit 2+ products are widely used for the SIM chips embedded in mobile phones. This technology is used to support the mobile solution for electronic IDs and electronic signatures supported by the ZebSign ID service. Entrust worked closely with a number of third-party suppliers, as did ZebSign through its parent company, Telenor Mobile Communications, in order to address compatibility issues between SIM chips, mobile phone "micro"-browsers and the GSM mobile phones themselves.
- There are future plans for the ZebSign ID service to support WAP- and UMTS- enabled phones in which alternative technologies other than SIM chips are used. For example, there is the possibility that the electronic ID functionality may be able to be downloaded as a Java applet to a wireless device using short messaging service (SMS). This is a possible solution suitable to the WAP environment and does not use SIM Tool Kit 2+ technology. Such forward compatibility with WAP-enabled devices will need to be provided through close coordination between suppliers, like Entrust and ZebSign.
- The ZebSign ID services run on a UNIX® computing platform comprised of multiple Sun Enterprise servers using the Solaris Operating Environment, Sun's version of the UNIX operating system.

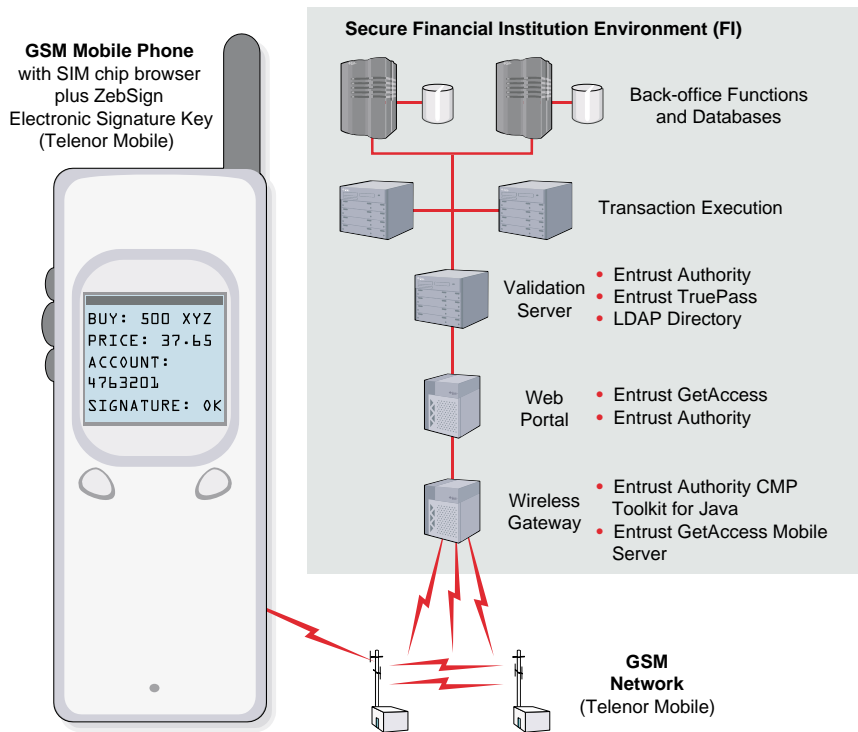
Alternative implementations of the ZebSign ID service described in the next section of this report show how the Entrust enhanced Internet security products are used by ZebSign to enable a more comprehensive environment of trust for eCommerce and mCommerce businesses.

Implementation of the ZebSign ID Service

Originally, Telenor ZebSign (prior to the foundation of the new Telenor and Norway Post ZebSign) planned to focus on mCommerce services. That was the area in which they had a unique market advantage and would get the greatest amount of attention, an important factor for a new technology initiative. However, delays in the availability of production quantities of SIM cards as well as the availability of the groundbreaking Entrust TruePass product led to a change in ZebSign's market entry focus. Using the Entrust TruePass product, ZebSign could begin targeting the traditional PC eCommerce side of the market. The ZebSign market entry solution would use a non-SIM feature of Entrust TruePass product to provide an out-of-band short message service (SMS) used in delivering a randomly generated one-time PIN to the PC user's GSM mobile phone for high security application access to server-based Entrust TruePass user profiles. Thus, market entry addressed both the Internet and wireless network environments and demonstrated the flexibility of the ZebSign solutions.

The PIN delivery via GSM mobile phone, developed by Entrust for ZebSign and now available through Entrust as a product called the **Entrust Mobile ID Server**, received considerable favorable comment because it addressed the concerns being published in Nordic newspapers regarding the security threat of PC memory sniffing in eCommerce. The one-time PIN is used to authenticate the PC user before giving access to the Entrust TruePass user profiles and, indirectly, access to only those eCommerce applications authorized for that user. As it is a one-time password or PIN, this lessens the danger of reuse or spoofing by an unauthorized user. And it is remarkably fast - ZebSign tests have shown transfer times less than three seconds from anywhere in Europe.

Figure 3: Example Future Environment for ZebSign Electronic Signing of mCommerce Transactions



Customer of ZebSign, Telenor Mobile and Financial Institution

Sample Transaction Sequence

- 1 Customer logs on to FI portal using ZebSign Electronic ID + name & FI account number
- 2 Customer orders 500 shares of XYZ
- 3 Customer electronically signs the transaction to confirm and execute the order
- 4 Wireless Gateway receives the signature, matches it with the certificate and conveys both the signature and the certificate to the Web Portal
- 5 The Validation Server retrieves the transaction from the Web Portal, validates it and clears it with the appropriate financial institution, archives the binding record of the transaction with a local time stamp and conveys a result-of-transaction record to the financial institution's Backend System

The out-of-band approach to one-time PIN delivery for secured eCommerce is illustrated in graphic form in Figure 1. (And it is also a key part of a real-world banking solution described later in this report.)

When the SIM 32KB chip with an on-chip co-processor became available in production quantities, ZebSign expanded their ZebSign ID service, making it possible for users to store their ZebSign ID on the mobile phone as well. This introduced a full PKI infrastructure for mCommerce. The implementation of ZebSign's mobile solution is shown graphically in Figure 2, which also identifies other key components that may be found in mCommerce solutions using the ZebSign ID service.

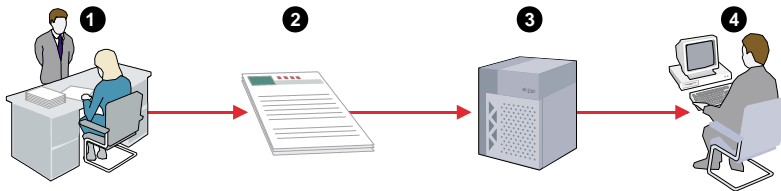
In addition to authenticating the end user with an electronic ID, the ZebSign

mCommerce solution can also be used to apply an electronic signature to an online transaction, a capability that is key to market acceptance (and regulatory requirement compliance) for online wireless transactions such as stock purchases. After initial log-on, validation and transaction authorization, the end user and the seller (e.g., banking organization or brokerage firm in the case of a stock purchase) step through a secured transaction to define the purchase to be made. The transaction then becomes an order and is executed only after the end user (buyer) appends an electronic signature. In figure 3, an example of how a financial institution or security firm might make use of the ZebSign ID service is illustrated with the Entrust TruePass software, involved in applying an electronic signature.

The above applications of the ZebSign ID service illustrates the basic capabilities. Other usage alternatives include:

- Authentication of a secured PC session on the SIM-enabled GSM phone. This is similar to the market entry solution illustrated in Figure 1 but employs the SIM chip in the mobile phone rather than a server-generated one-time PIN sent to the phone using SMS messaging.
- Signing a document that is on the PC using the SIM-enabled GSM phone as the electronic signature source. This solution employs a 'fingerprint' algorithm on the PC, which is sent to the PKI server where it is associated with the user's GSM mobile phone. The server then sends the fingerprint in encrypted form to the GSM phone where the electronic signature is applied to the fingerprint and both are time-stamped. The fingerprint and secured document are then combined as a signed document at the PKI server level. The goal is to use the highly secure SIM card as the source of the electronic signature rather than a less secure software-based PC. A second goal is to avoid the use of a smart card at the PC, due to user costs and other usage complexities

Figure 4: ZebSign ID Registration and Activation Process for a New Subscriber to Internet Bank Services



Financial Services Example of the ZebSign ID Service in Practice

The following example illustrates how the ZebSign ID service supports both current and future requirements in the financial services sector. This example covers the registration process, with either ZebSign or a financial institution serving as the registration authority; use of the out-of-band one-time PIN process (illustrated earlier in Figure 1), and the use of the ZebSign ID as the basis for user access control to selected Internet banking services. A user will register to the financial service, e.g. Internet banking service, with the conditions that the service requires an electronic ID from ZebSign. Users that already have a ZebSign ID can sign the conditions for using the banking service directly on the Internet and start using it immediately.

The registration process for new subscribers is comprehensive, but simple and virtually transparent to the user - all as a result of the combined business and technical expertise applied by ZebSign with assistance from Entrust. In this example, users that do not have a ZebSign ID will be prompted to confirm some personal data online and upon doing so, a personal activation code will be generated. The user will then be issued an SMS via mobile device, advising the user to pick up his or her activation code at a nearby bank or post office that the user selected during the registration process. After proper identification and signing the conditions for using ZebSign ID, the user will then receive the activation code. The final step of this process is a simple activation process online through a dialogue with Entrust Authority Self Administration Server module of the ZebSign ID service. The user can now begin using the ZebSign ID, to conduct online banking along with many other services.

The registration and activation processes are illustrated in Figure 4.

Once activated, the ZebSign ID service provides a Secure Web Portal with single sign-on for registered bank customers as well as complete enhanced Internet security for the bank. Sign-on and authentication via the Internet proceed in

- 1 An existing bank customer decides to subscribe to Internet Banking Services and obtains registration procedures and guidelines from the bank.
- 2 Customer completes and signs registration application form in person at bank office. (Alternatively, the registration process can be done at any Norway Post branch office, or by Registered Mail to ZebSign.)
- 3 The registration information is processed off-line and, if approved per bank criteria, a new user profile is established for the new subscriber. The new and still inactive profile is stored by Entrust TruePass at the ZebSign CSP facility. The customer is informed by email, post or phone that their user profile has been generated and they can now activate their account.
- 4 The customer activates their account by registering online at any time through a menu-guided dialogue using the Entrust Authority Self-Administration Server module at the ZebSign CSP facility. Once activated, the customer can thereafter use the ZebSign ID for authentication and access to Internet Bank services. (See Figure 5 below.)

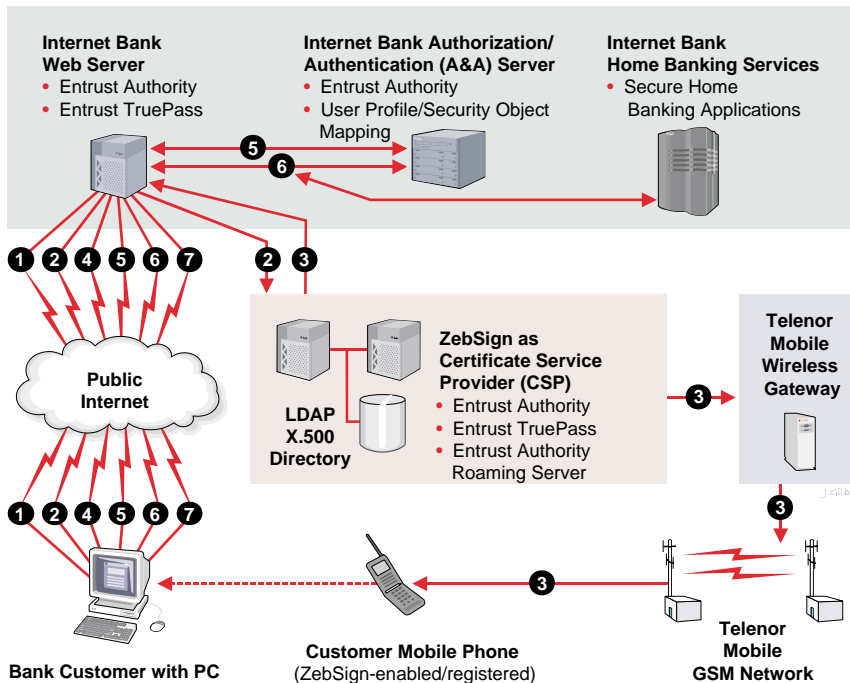
- The ZebSign ID service may in the future also support the mCommerce WAP environment with or without the use of SIM cards as storage for electronic IDs. The WAP environment encryption service, wireless transport layer security (WTLS), will then be supported for mCommerce in the same manner that SSL is used in most eCommerce solutions today.
- The ZebSign ID service includes gateway facilities between GSM wireless networks and the Internet for access to the Web sites of supported businesses and their service providers.

Secure Registration: A Key Part of the ZebSign ID Service

In order to obtain electronic signatures on transactions and to help meet the requirements of the authorities regarding money laundering, the usage described above must be preceded by thorough registration including face to face identification of all users. ZebSign has put a huge effort into engineering efficient procedures, agreements, support systems and policies to meet even the most stringent regulatory requirements, yet being simple and understandable for the end users.

The ZebSign ID service may use a variety of registration authorities, ranging from banks to post offices. All registration points must have proven security and follow procedures that have been accepted by the authorities. The user must participate in person at some stage in the registration process. When properly registered, the user may activate his or her certificate in a Web dialogue with the PKI through the Entrust Authority Self-Administration Server module. The resulting electronic ID is recognized and accepted by all parties based on the ZebSign ID certification policy.

Figure 5: Example Architecture with ZebSign as CSP for Banking Web Portal



via the PC and log-in to the secured banking application is complete. (This is a very successful application of the out-of-band one-time PIN feature described earlier in this report and illustrated in Figure 1.)

The remainder of the transaction, until sign-off, is directly between the customer's PC and the bank applications servers and databases.

This example of ZebSign ID in practice is shown graphically in Figure 5.

This example in Internet-based home banking meets the key criteria established by ZebSign when it embarked on the ZebSign ID initiative. These include: *no cost to end-user (bank's customers), simplicity, higher level of security than accorded by software-based certificates at the PC, cross-channel integration and everything is done within a comprehensive PKI-based environment of trust.*

ZebSign Current Status and Future Outlook

The present ZebSign organization, owned jointly by Telenor and Norway Post, came into being in 1st Quarter 2001 and merged the prior work and facilities from the founding organizations. These included:

- April 2000: the first mobile electronic signature using SIM Tool Kit 2+ mobile phones as storage for the electronic ID was demonstrated in the Telenor Mobile laboratories.
- May 2000: Telenor Mobile selected and made arrangements with a leading Norwegian bank to be the first ZebSign ID customer.
- June 2000: the on-going technology co-operation between Telenor and Entrust was formalized by signing an Enterprise/CA Service Provider License agreement.
- September 2000: the market entry of ZebSign ID service using the Entrust TruePass capabilities for network-centric authentication (before the availability of

Session 1 Sequence (Log-on to Authentication)

- 1 User connects to the Bank's Web Server protected by Entrust TruePass.
- 2 Bank's Web Server contains Entrust TruePass extensions that download Java applet prompts to user PC requesting name and password; user enters and transmits name & password. Bank Web server transmits user name to Entrust Authority Roaming Server (at ZebSign CSP site).
- 3 The Entrust Authority Roaming Server looks up Entrust TruePass profile stored in encrypted form and sends it to Bank Web Server. Concurrently ZebSign's PIN Application Module generates a one-time PIN that is transmitted (a) to the user's mobile phone in SMS text form and (b) to the Bank Web Server in hashed form.
- 4 The Bank Web Server prompts the user PC for the PIN; the user enters the PIN and it is sent in hashed form to the Bank Web Server.
- 5 The two hashed PINs are compared at the Bank Web Server and, if equal, the encrypted Entrust TruePass user profile is downloaded in the secure Java sandbox in the user's PC browser. Here it is decrypted and automatically performs strong user authentication through the Bank Web Server to the Bank A&A server. The Bank A&A Server also maps the Entrust TruePass profile to the Home Banking Security Objects and determines if user is authorized to perform requested home banking transaction. If yes, secure Session 2 is initiated.

Session 2 Sequence (Home Banking Transaction Execution)

- 6 Authenticated/authorized customer gains access to home banking applications; customer proceeds through transaction execution; if transaction requires electronic signature(s), the customer can use the certificate stored in Entrust Truepass to electronically sign and execute the transaction.
- 7 Customer logs off at end of secure home banking transaction execution.

the normal process (user ID plus strong password plus 128-bit SSL support), setting up a secured session for banking transactions. However, the next step differs substantially from the traditional Internet banking sequence. The ZebSign ID service consults the Entrust TruePass user profile for the bank customer and determines that the customer is authorized to access the requested service *subject to separate out-of-band authentication* via the customer's GSM phone. The ZebSign PKI server generates a one-time PIN and sends it to the customer's GSM phone. The customer then enters the PIN

ZebSign expects customer growth to reach 200 - 300% by 2003 and to continue this growth pattern into 2004.

production quantities of 32 KB SIM chips with on-chip co-processor) was demonstrated and released.

- April 2001: ZebSign electronic IDs were used by thousands of Norwegian taxpayers filing their tax return forms.
- June 2001: The "SmartPay" system was piloted among a substantial user community. SmartPay is the first commercially available service based on on-chip electronic signatures from Telenor, where any mCommerce portal can have transactions accepted and signed by any Telenor Mobile user. The result is accepted by the banks for clearing funds between the parties.
- August 2002: The ZebSign ID service was expanded to also cover smartcards as storage for electronic IDs (Now covering SIMcards, smartcards and netcentric storage). After a long pilot period with a couple of thousand users, the solution went into production. The first service provider using this solution with the ZebSign ID service, used it to facilitate electronic betting by paying for it, checking the coupon and collecting the prize money. There are also local counties in Norway preparing to make use of this solution for official application treatment. This way of storing the electronic ID is targeted towards service providers required to conform to the standards of qualified signatures brought forward by the EU (European Union), requiring the use of a secure signature creation devices. The ZebSign ID service support qualified certificates, but the smartcard used as storage is not yet evaluated according to the standard for secure signature creation devices, to give qualified electronic signatures.

Within the new ZebSign organization, the ZebSign ID service is being refined constantly and rolled out to customers as development work on new and expanded solutions continues. ZebSign is working closely with their partners delivering electronic IDs for all variations of access devices. In the first phase of contact, the expectation is for users to view the ZebSign ID as a single service provider solution. As consumers start using several different services, the simplicity ZebSign introduces will be apparent, having one security solution for all services. Expansion into other remote user access devices such as home TV, personal digital assistants (PDAs), vending machines and game/entertainment devices is expected in the future, beginning with digital TV and PDAs - launching soon to be supported through the existing solutions, according to the PDAs growing capabilities.

Today's status of the ZebSign ID service can be summarized as follows: The ZebSign ID service provides a closed environment for a community of Scandinavian end users and service providers. However, the solution has been prepared to meet European Union (EU) laws and regulations and to be compatible with the ETSI "Qualified Certificate" standards. This will allow ZebSign to engage in pan-European operations. In addition, these and other advances will position the ZebSign ID service to meet the Identrus standards (already supported by the Entrust products) and open the broader banking community for ZebSign ID usage. (See Glossary of Terms for more information on Identrus.)

Concluding Observation

The unique circumstances of the Norwegian market with respect to voice telecom services, GSM wireless services and Internet services offer an ideal test bed for the development, deployment, production use and evolution of enhanced Internet security solutions for eCommerce and mCommerce. Telenor, the leading telecom, IT and media company in Norway, working with Entrust, developed a family of electronic ID solutions and put those solutions into production use in less than one year, making the ZebSign ID service.

The recent expansion of ZebSign as a joint venture owned by Telenor and Norway Post, assures continued development and support for this highly innovative electronic ID approach. The relationship between ZebSign and Entrust, provides a comprehensive environment of trust for eCommerce and mCommerce in Norway and the Scandinavian countries, and also provides a foundation for further expansion of ZebSign ID services to a larger geographical area.

Glossary of Key Terms

CA	Certification Authority: The system responsible for issuing secure electronic identities to users in the form of certificates. With Entrust enhanced Internet security products, the Entrust Authority™ Security Manager product serves as the CA.
Certificate	A secure electronic identity conforming to the X.509 standard; typically contains a user's name and public key. A CA authorizes certificates by signing the contents using its CA signing private key.
Digital ID	A Digital ID is an encrypted repository containing security data that is unique to an individual in a PKI environment. It includes the private keys of that individual and can only be accessed via an authentication scheme that employs some combination of tokens, biometrics or passwords. A Digital ID is not the same as a Digital Signature (see below).
Digital Signature	Performs the same functions as a paper signature except that it is fully electronic. It is currently computationally infeasible to forge a digital signature, making it more secure than a paper signature. A digital signature provides the recipient with a means of verifying that the signed content (e.g., data file) came from the person holding the private key that signed the document, and that it has not been altered since it was signed. Digital signatures are becoming increasingly recognized by governments, including the U.S. government as legally recognized signatures. A Digital Signature is not the same as a Digital ID (see above).
Electronic ID	<i>In this Case Study, the term "electronic ID" is used in accordance with Norwegian market terminology. An electronic ID in this case, is the electronic identity of the end user that can contain one or more digital IDs. These digital IDs can be stored differently, for example, on a smart card, SIM card, or in a netsentric profile server, but can always be identified as a part of the electronic ID through the unique end user name. With the electronic ID, a service provider can identify the end user regardless of which digital ID is used, delivering a personalized service independent of the network or token used to access the service.</i>
Electronic Signature	In this Case Study, the term "electronic signature" is used in accordance with Norwegian government guidelines. Any reference to an "electronic signature" in this study is specifically referring to what Entrust terms as a "digital signature"- see glossary definition of "Digital Signature" above.
ECC	Elliptic Curve Cryptography, the type of public key cryptography used for encryption for the Wireless Transport Layer Security (WTLS) methodology used in secured WAP-enabled wireless communications systems. ECC is not compatible with SSL encryption, thus requiring a conversion step for secure message exchanges between wireless solutions and Internet-based systems. The required conversion process renders the message insecure for a brief time period (milliseconds) in the end-to-end message exchange process.
GSM	Global System for Mobile communications is the standard for wireless transmission and switching operations in most of the world outside North America.
Identrus	The Identrus system, initiated by some of the world's largest banking organizations, provides a set of standards and an infrastructure for eCommerce trading partners. The Identrus infrastructure depends on PKI-based technologies that include crypto-secured digital identities and realtime validation of those identities. Identrus is administered by Identrus LLC. (See www.identrus.com).
LDAP	Lightweight Directory Access Protocol is specified by the IETF RFC 1487 standard and is the most commonly used protocol for access to authentication directories in PKI security systems. It is a standard used for the Entrust family of PKI products.

Roaming	In a wireless PKI environment, the term 'roaming' refers to the capability that allows a user to move from one device to others in the same PKI domain without any need to take along any Digital ID equipment, software or tokens for authentication purposes. Device independent and location independent 'roaming' is a key feature of the ZebSign Generic ID solutions.
SIM	The Subscriber Identification Module is a chip in a wireless device such as a mobile telephone that is programmed by the issuer to include information unique to the user. This includes subscriber information for tracking, billing and related purposes, storage of frequently used telephone numbers and applications like simple "micro"browsers and, in a PKI environment such as that employed by ZebSign, also includes a Digital ID unique to the user. SIM chips have become increasingly powerful as the use of wireless communications systems for data purposes has expanded dramatically. Today's SIM chips have 32 KB of programmable memory.
SIM Tool Kit Phase 2+	This is the set of tools used by issuers of wireless devices for programming SIM chips to provide both generic capabilities (e.g., micro-browser) and unique identification (Digital ID) for a device to be issued to a user.
SSO	Single Sign-On is a methodology used to allow users accessing a Web site portal to log on only once and with one Digital ID regardless of the number of URL destinations within that Web site to be accessed. The Entrust GetAccess™ product is a leading solution for SSO capabilities.
SMS	Short Messaging Service is a standard for packaging and managing short data messages, usually less than 80 characters in length, for both terrestrial and wireless telecommunication systems.
SSL	Secure Sockets Layer is a secure session protocol specified by Netscape Communications and widely used in Internet-based messaging systems for secure communications between remote clients equipped with industry standard browsers and selected Web-based services.
UMTS	UMTS (Universal Mobile Telephone System), is a third-generation mobile telecommunication service based on wideband code division multiple access (W-CDMA) technology. UMTS enables telecommunications service providers to offer high-speed multi-media applications to mobile subscribers. Telenor Mobile Communications holds a UMTS license for Norway.
WAP	Wireless Application Protocol is a widely accepted standard for enabling wireless devices such as mobile telephones and portable digital assistants (PDAs) for handling data as well as voice messages.
WTLS	Wireless Transport Layer Security is the encryption methodology used for wireless data messages and performs the same functions in a wireless network as does SSL for Internet-based security. It employs the ECC encryption methodology. (See above)
X.509	X.509 is the internationally accepted standard for Certificates used in PKI security systems.

About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world leader in securing digital identities and information, enabling businesses and governments to transform the way they conduct online transactions and manage relationships with customers, partners and employees. Entrust's solutions promote a proactive approach to security that provides accountability and privacy to online transactions and information. Over 1,200 enterprises and government agencies in more than 50 countries use Entrust's portfolio of security software solutions that integrate into the broad range of applications organizations use today to leverage the Internet and enterprise networks. For more information, please visit <http://www.entrust.com>