



have recognized that the cards are an excellent option for storing additional security and commerce applications.

Supporters claim that storing digital certificates and signatures on smart cards will be more secure, portable and convenient for consumers than storing them on the mobile device. One drawback, though, is that mobile phones and handhelds are not equipped to handle the cards. Mobile phones will require dual slots, and PCs, laptops and handhelds will need a smart card reader.

Instead of requiring a new round of dual-slot phones, PKI applications could reside in a mobile phone's SIM or Wireless Identity Module. Multiple private keys could be stored on the SIM, but it is highly unlikely that financial institutions will put their customer information on a card or a device managed by the service provider. Instead, banks, financial institutions and possibly retailers will issue their own smart cards with embedded customer identities. In this m-commerce vision, consumers will carry multiple smart cards with separate digital identities in their wallet.

#### Certificate authorities own PKI center stage

Whether PKI is embedded in the SIM, included on a third-party's smart card or added within the mobile devices, consumers and merchants will rely on the certificate authority (CA) to validate each m-commerce transaction. The CA plays the integral role of trusted provider of the encrypted keys. It is responsible for exchanging the keys securely, and it authorizes and authenticates the merchants and buyers.

Each party enters a transaction relying on the certificate authority, which issues the public and private keys. These CAs are entrusted with validating each consumer and maintaining a record of each key exchange. Different groups—banks, mobile operators, retailers—are considering taking on the role of CA. In that capacity, each would control one more aspect of the m-commerce value chain.

Financial institutions have banded together to form Identrus to enable secure online transactions. The group sees itself as the logical choice to act as the CA and is working to define standards and business models for Internet commerce. Although many expect financial institutions to fulfill this role, industry watchers predict that carriers could also offer the service.

"Carriers acting as CAs could issue certificates on a smart card or in the phone. They could control every aspect of m-commerce, because they control the network," says Peter Quadagno, president of Quadagno & Associates, a consulting firm that monitors smart card development worldwide.

Most likely, though, the market will have multiple CAs. "We won't have just one CA. It could be the mobile provider, a portal provider, a bank, or Sears," says Mike Lancas, product manager at Marconi Services.

With multiple CAs, each one would be responsible for different transactions. "A mobile operator may issue a certificate that would allow an end user to buy small items like movie tickets, books or CDs. For higher value transactions, the certificate would probably come from Visa or MasterCard," says Paul Healy, vice president of wireless services at VeriSign. "Charles Schwab or other financial institutions would offer a certificate for stock transactions."

Of all these players, mobile providers are probably the best equipped to take on this role. They have the network infrastructure, the

personnel and the data centers, says Kevin McBride, vice president of application development at iSoft. "A service provider's data center is the logical place to host a CA. They have invested in massive, secure IT infrastructures, which is exactly the type of environment necessary to host a trusted security authority."

Cingular is already targeting m-commerce services by 2003. "We are increasing our back-office security and developing partnerships with banks to develop m-commerce options," says Dave Williams, vice president of strategic planning at Cingular.

Both VeriSign and Entrust have mobile operator customers conducting pilot programs using PKI. The carriers have been concentrating on offering certificates for Web sites and signatures for e-mails. VeriSign is working with BT, Telia and Telephonica, and Entrust is helping Norway's Telenor Mobil. In some cases, mobile operators outsource the CA responsibilities to third-party companies. Alternatively, the operators could choose to set up shop as a CA or create a separate division. BT has created BT TrustWise, and Telenor Mobil has formed ZebSign with Norway's postal service (see sidebar, "Norway's PKI Plan," page XX).

#### Outsourcing vs. in-house support

To become a CA, the applying company is put through rigorous tests to ensure that it can guarantee its customers' identities, protect the users' data, and reliably decrypt and encrypt information. Each country has its own set of policies and requirements; typically a CA can only issue certificates for the country where it is located.

If an operator chooses to go through the testing process and support a CA in house, it will need to invest in equipment and personnel. Equipment costs include redundant servers to run the software for the cryptography of the root certificates and the authentication of the users, as well as a secure vault. This private vault has three to four layers of security to protect customer data.

Before the customer data can enter the vault, the CA has to qualify each customer and ensure that the identities are factual. The CA must guarantee that the digital identity corresponds with the correct customer. And, once the transactions begin, the CA must have a rigid auditing process to track each the customer's activity.

Equifax Secure puts the initial costs of bringing up a CA at between \$5 million and \$7 million. While building the infrastructure is expensive, Marconi says another cost is the resources necessary to manage the service. "The cost isn't in the security software. The costs will come from registering the users and validating who they are," says John Dale, chief operations officer for Marconi's SecurTrust. "But providers have the infrastructure and the resources in place to handle these tasks."

Rather than building and supporting the back-end PKI systems, mobile operators could choose to outsource those functions and limit their responsibilities to maintaining the front-end registration process. In this scenario, they would sign up customers for a certificate and validate customers through their subscriber database—and let a third party do the heavy lifting on the back end.

"Sharing front-end and back-end responsibilities is one of the best ways to test CA programs," says Carl Stucke, chief scientist at Equifax Secure. "Operators let someone else handle the cryptography, and they don't have to bear the financial or manpower expense of building a public key infrastructure. Later, if they want, they can bring the process in house."

Entrust agrees that outsourcing has multiple benefits but expects that carriers will not take advantage of them. "Outsourcing can save expenses and help operators get to market quickly, but the biggest disadvantage is that it gives away control. Telcos like to control their business and keep everything in house," says Richard Kirk, vice president of Entrust's worldwide wireless division. VeriSign's Healy breaks the decision down to the operator's culture and size. If the carrier's business model is built on outsourcing, it will choose the outsource option. Or, he says, it could depend on the subscriber base. "Smaller carriers, with only 1 million or 2 million customers, could find it very expensive to support a CA in house. Carriers with more than 20 million customers will probably run it themselves."

Another consideration is the carrier's reputation in the community. "Smaller carriers will have difficulty convincing customers to use their certificates. Customers would be more likely to use a company that is more recognized and trusted," says Dave Smith, director of market development at ACI Worldwide, an international provider of electronic payment solutions.

Not everyone agrees that only well-known names will succeed. "The bigger companies won't be the only CAs," says Robert Lendvaid, vice president of marketing at KyberPass. "Smaller companies may want to offer certificates as a value-added service."

#### Security, accuracy, reliability

For carriers that decide to limit their responsibility to registering customers for a digital certificate, VeriSign offers an outsourcing service that deploys servers and software to a carrier's data center. The server is securely connected to VeriSign's Mountain View operations center to transfer approved customer information.

To sign up for digital certificates, customers should have multiple options. They may be able to obtain one when they purchase the phone, order one over the phone, or request one through a Web site. If registration is available through the mobile operator's Web site, the customer would identify himself through an account number, PIN, address, Social Security number, or a combination of information. This data would be compared to the operator's subscriber base, and once the customer is identified, the server would check the subscriber's credit. If all is approved, the server passes the request to VeriSign to issue the certificate. "The carrier just needs to make sure the server at its site doesn't fail," adds Healy.

However, Healy warns, the carrier is responsible for authenticating the customer and ensuring that the address, name, phone number, Social Security number, and other details are correct. "If the carrier does not trust its customer data or can't authenticate its customers," he says, "it could work with companies such as Lightbridge to improve its systems. This data must be accurate to ensure security and lessen the risk for fraud."

Entrust's Kirk expects that billing systems will be highly integrated with the PKI infrastructure to compare digital signatures and to ensure nonrepudiation. "If an operator is using the billing system to validate customers, it must have verification for legal purposes," Kirk says. "In an m-commerce world, problems will be magnified."

Cingular's Williams agrees that the process will be complicated: "We must be assured that we are sending the right information to the CA system and that we're sending it securely. Tunneling protocols may be the key to adding security layers to this data transfer."

#### Managing m-commerce momentum

Even with promises of high-security vaults and rigid accounting procedures, PKI providers recognize that their role in m-commerce's future is unclear—as is m-commerce's future. Just as e-commerce has become tarnished, m-commerce could fall from grace.

Entrust, VeriSign and the others predict the next six to nine months will be a critical period. During this time span, they expect more decisions will be made about appropriate applications, standards and technologies. And the market will determine who will play the leading role in the m-commerce supply chain.

Although financial institutions continue to get the first reference as CAs, carriers are also seen as potential players. Whether carriers will accept that responsibility is unclear, though. "Service providers have to say they want to be in payments," says ACI's Smith. "So far, they haven't openly shown that they want to be involved."

Some type of involvement from carriers will be required. The transactions will pass over their networks, and PKI will play a part. While the business issues are being resolved, the PKI providers urge carriers to strengthen their security knowledge, so that they can expand their role beyond network provider.

"Many m-commerce issues are debatable at this point, but it's commonly accepted that PKI is the fundamental building block to enabling mobile transactions," says Entrust's Kirk. "The technology is being written into standards and is widely accepted by the community. What is debatable is how well the telcos will understand PKI and be able to integrate it within their systems."

[sbar]  
Norway's PKI plan

PKI is gaining support in Norway through ventures such as ZebSign, a joint company that grew out of Telenor Mobil and Norway's Postal Service. At ZebSign, Norwegians will be able to register for a digital identity that can be used on all of Norway's networks and terminals. The ID will be encoded in a SIM card on the mobile phone or stored on a PC or smart card.

Before launching ZebSign, Telenor Mobil and the Postal Service had been building separate public key infrastructures. The two groups decided that pooling their resources and dividing PKI responsibilities would better serve Norwegians. Each would control the aspects of PKI that reflected their core knowledge base.

The Postal Service will assign, verify and maintain the registration of the digital identities, and Telenor will provide consumers with the access channels, infrastructure and applications that enable online commerce.

Pull Quotes

"A service provider's data center is the logical place to host a CA. They have invested in massive, secure IT infrastructures, which is exactly the type of environment necessary to host a trusted security authority."

Kevin McBride, iSoft

Many m-commerce issues are debatable at this point, but it's commonly accepted that PKI is the fundamental building block to enabling mobile transactions.

Richard Kirk, Entrust