JAVA AND THE NEW ERA IN SMART CARDS

By Dan Balaban

What you need to know about the far-reaching changes the industry has in store for its popular software platform – and for the smart card itself.

In the growing family of IT devices, the smart card is but an orphan.

While desktop PCs, laptops, handhelds and cell phones are more and more linked by the Internet and broadband communication, the lowly chip card speaks a language all its own and sends and receives data at snail-like speeds.

The one thing it does better than other devices is security, which makes it a natural for controlling authentication, payment and rights for downloading music, games and videos in an increasingly networked world. But since the smart card requires a burdensome infrastructure of drivers, special hardware and middleware just to communicate with other devices, it risks being bypassed even as the need for data security grows.

"Orphan? It's worse than that; it's like a caveman living in the 21st century," says Gary Waite, a former smart card industry executive, now Java SIM products development manager with UK mobile operator O2.

If true, then the smart card industry is starting to emerge from its cave.

Industry executives have launched several initiatives they hope will secure the future of the smart card. Among them is a nearly 20-million-euro three year project funded in part by the European Union to develop a new generation of smart card technology to allow people to stay connected securely and seamlessly on a range of portable devices.

Major vendors are also perfecting the "network smart card," a concept that has been floating around the industry for years. It puts the Internet protocol stack onto the card, allowing it to talk as equals with servers and PCs online – only the smart card will be the secure party to the conversation. Two major vendors plan to market a network smart card by next summer.

But arguably, the most significant work is being done by the Java Card Forum and Sun Microsystems, the owner of the Java Card platform and ultimate arbiter of the Java Card smart card specification. Together, they plan to introduce a next generation Java Card by 2007.

The so-called "Java Card 3," sometimes called JavaCard.Next, would remake the industry's most popular software platform to allow smart cards to hold their own with other IT devices, especially the proliferation of more sophisticated handsets that also run Java.

With the platform, sometimes also referred to as "Java Card 3.x," because it would follow the current 2.x series, smart cards could run more than one application at a time and plug directly into handsets and PCs with no additional software needed on the larger devices.

A user, for example, could download a game onto his handset and pay for it at the same time, while keeping the phone's voice channel open. Or he could point his handset browser at a secure Web page stored directly on the phone's subscriber identity module smart card, or SIM, putting the dull SIM toolkit user interface to shame.

A consumer shopping on the Web could link his card directly with a merchant server, bypassing the PC, except to use it as a dummy terminal on which to type commands. A simple USB connector to the PC would be all that is needed if the PC doesn't already have a smart card slot.

The card could do this because it would support TCP/IP and other Internet protocols.

"I can put the card into any computer, a PDA and into any mobile, over time, and have it fit and work without software on the host," says Bertrand du Castel, director of research for France-based vendor Axalto and head of the Java Card Forum's technical committee. He supervised work on the first Java Card before it was introduced in 1996.

Castel and other backers of the next-generation Java Card say chips will be available in the next couple of years to support the new initiatives. That includes those packing sufficient random-access memory, or RAM, to allow card-holders to run several applications at the same time.

While other types of memory on the smart card, as well as processing power, have roughly kept pace with the rest of the IT industry, the problem has been that the basic protocols smart cards use to communicate and download data haven't changed in 15 years. At that time, mere bytes of RAM were available to smart card developers.

Opening the Bottleneck

While demand for smart cards continues to grow, these limitations have consigned the cards largely to the role of a simple authentication or identity token and small data carrier, used by mobile network operators, banks and some government agencies and corporations. This is fine foe many issuers, such as banks, which mainly want a tamper-resistant card on which to store account information and encryption keys.

Others want more. But besides its poor communication and downloading skills, the smart card has other problems relating to the IT world. The arcane communication formats and languages the smart card uses – known as the "7816" protocols for the main international standard that governs contact chip cards – make it difficult for developers to write applications. That's why, despite earlier promises of Java Card promoters that the platform would open up smart cards to a pool of millions of Java-savvy programmers, application development is still almost exclusively the domain of card vendors.

"You need special expertise to develop software for that (smart cards)," says Michel Koenig, who teaches smart card technology and application development at the University of Nice in Sophia Antipolis, France. "By using TCP/IP, there is no need. They (programmers) can use their own knowledge of software."

But not everyone supports the idea of such a sharp departure from the current generation of Java Card, which was proposed by the Java Card Forum about 18 months ago. The forum, drawn from representatives of the licensees of the software, takes the lead in writing specifications. It is headed by major card vendors, which pay the bulk of the royalties to Sun.

In fact, Sun was against the idea for Java Card 3 and wanted to continue the present series longer, sources say. It only signed on in June. Sun was concerned about the expense and possible confusion in the market that maintaining separate old an new platforms would create. Then there was the issue of backward compatibility – to what

degree card issuers will be able to run current Java Card applications on the new cards.

This is still a major concern for supporters and critics alike. While Sun and the Java Card Forum have promised the next generation Java Card will be backward compatible, they have not agreed on just how they will accomplish this or how much the new platform will add to the cost of cards.

"Backward compatibility is critical," says Robert Brandewie, director of the Defense Manpower Data Center, which has issued 5.5 million ID cards to employees of the US Department of Defense and related personnel – all of them supporting Java Card.

But Brandewie also sees the potential benefits of the new Java, including eventually doing away with the extra software the DOD has had to load onto every card-holder's PC, which enables the card to control network access, its main function. This would save the department millions, and make adding new applications and changing vendors much easier.

Banks are expected to be the strongest opponents of the new Java Card. They have complained in the past that the software platform is changing too quickly. For example, they generally opposed the move two years ago to Java Card version 2.2, which made application writing easier and improved interoperability among cards from different vendors. That revision also had a feature called remote method invocation, or RMI, which helped clear the way for issuers to link Java applications on the SIM card with those on other devices, such as mobile phones.

The banks developed their applications on the preceding version, Java Card 2.1, after which they put the cards through a rigorous security certification process required by their card organizations, Visa International and MasterCard International. They didn't see any need for a new version, which, if they moved to it, would force them to redevelop the applications and go through stringent security checks again. The impact would be even more dramatic with the next-generation Java Card.

"There are different views of how fast and how radical the change needs to be," says Marc Kekicheff vice president of emerging technology for Visa International. "We don't see any urgency to change anything."

Kekicheff is also technical director for GlobalPlatform, an industry group seeking to promote rollouts of multi-application smart cards. Visa developed the mechanism used by Java Card for the secure download of new applications to cards after issuance, and later donated the loader to GlobalPlatform. There are also concerns that this loading mechanism would be changed in Java Card 3, forcing mobile network operators and other issuers to redevelop their over-the-air platforms used to download data to subscribers' handsets.

Architects of the new Java Card say they see no problem keeping the GlobalPlatform loader intact, which is reassuring for Kekicheff. "We're perfectly okay, as long as we can run GP (the GlobalPlatform loader) on top of it," he says.

Visa played a major supporting role in the mid-1990s in the creation of the first Java Card. That is ironic, since today relatively few Visa member banks issue Java cards or use GlobalPlatform software. Mobile network operators are the main consumers of the software, for their SIM cards, which represent the vast majority of the 750 million Java Cards that have been issued over the past seven years.

And it is the mobile network operators who are expected to be the biggest supporters of the new Java Card. Among the new features they look forward to using is multithreading – running more than one application at a time. This would give Java

Card more in common with immensely popular Java operating software used on may phone handsets and PCs.

Today, SIM cards can basically run just one application at a time. Although there are ways around this restriction, it limits the type and number of value-added services operators can offer on their SIM cards – especially since value-added services could interfere with the core function of the SIM, to authenticate subscribers to the network.

This problem could arise, for example, if a subscriber was downloading a ring-tone from his SIM toolkit menu at the same time the network is trying to reauthenticate the subscriber, as it occasionally does. If the networkjust happens to ask for the credentials of the subscriber's SIM during the ring-tone download, the subscriber could lose the network connection.

"we are clearly in need to have a processor and software in the card being able to run two to three applications at the same time," says Christian Goire, chairman of the Java Card Forum.

Multithreading will require that smart card chips carry much more random-access memory, which is the workspace the chip uses for processing applications. This is volatile memory, which means it only holds data and code while powered up by the reader. And it is also expensive. That is one reason today's high-end smart card chips carry no more than 8 kilobytes of RAM. They would have to offer at least 16K of RAM for the new Java Card, say some backers. But others, including some card vendors working on the new Java Card project, believe in order for the card to deliver acceptable performance, the requirement will be more in the range of 24K to 32K, even as much as 64K. Every additional kilobyte of RAM requires nearly four times the amount of silicon of a kilobyte of the standard non-volatile data storage memory used on smart card chips, EEPROM. Silicon is the biggest factor in the price of chips – the more silicon, the higher the price.

As for backward compatibility, the new Java Card would also have to support all the old application programming interfaces and other functions of the current Java Card 2.x series. There are no technical barriers preventing the Java Card 3 series from providing this; after all, the current version of Windows for PCs still supports old DOS commands. But it requires more space in the smart card chip's memory, although not in RAM. "Essentially, you'll be including a 2.x card inside your 3.x card," says Michael Montgomery, a scientific advisor at Axalto and head of a key subcommittee of the Java Card Forum dealing with communication protocols.

Some observers have their doubts the Java Card Forum and Sun will be able to pull off full backward compatibility, or if they do, it will be memory intensive and difficult to manage. Application programming interfaces for both new and old Java applications would have to reside on the same card. And, developers will have to decide how to convert the old Java Card files into the format the next-generation card would use.

But Peter Cattaneo, head of Sun's Java Card business, promises that issuers will not only be able to run their current applications on the new cards, they will be able to run their new Java Card 3 applications on the Java Card 2.x series. "We will be delivering backward compatibility," vows Cattaneo.

He an card vendors also say they will continue to support the current 2.x series Java Card for as long as issuers want to use it.

Architects of the new Java Card do not have estimates on how much more the chips will cost because the chips are not yet available. But for mobile network operators, who would likely be the first to rill out the new platform, backward

compatibility, and the corresponding costs, must be paid. Otherwise "it could be a problem for the (GSM) community," warns Sergio Cozzolino, director of the smart card services department at Telecom Italia Mobile and head of the Smart Card Application Group in the industry's major trade organisation, the GSM Association. "Otherwise, there would be no interest for us to upgrade."

TIM and the association, in fact, have called upon the smart card industry to bring its technology more in line with other IT devices, so they would welcome the proposed changes to Java Card. So does UK operator O2, which only issued its first Java SIMs last year.

Backward compatibility of the new and old Java Card doesn't have to be 100%, however, says O2's Gary Waite, who would be willing to redevelop his existing Java Card applications to run on the new platform. "We would do this because the benefits of the much more flexible system outweigh the costs of porting," he says. Waite notes that while Java Card 2.2 allows Java applications on SIMs and handsets to talk the same language, a special channel still has to be set up to make this happen. This is in the form of an application programming interface handset makers will need to add to their Java operating software – the now widely deployed J2ME (Java 2 Micro Edition). But while the API, called JSR 177, was added to the J2ME standard this past summer, manufacturers are under no obligation to implement it in their Java handsets.

The next-generation Java Card would make add-ons like JSR 177 unnecessary. Being able to communicate easily with handsets is critical for smart card vendors, who fear operators will more an more move their value-added services to platforms such as J2ME. That would relegate the SIM card to its old role of authentication, nothing more, not even security-based value-added services such as payment for mobile commerce or digital rights management for downloads of music, games and video.

"I think we have to be ambitious, we should compete with the J2ME platform…or collaborate," says Laurent Lagosanto, an engineer at Gemplus Labs, the research and development arm of the French based card vendor Gemplus International.

But the plans for integrating smart cards more closely with other IT devices go beyond Java Card, "it is more about the future of the smart card," points out Eric Alzai, chief technology officer for French-based Oberthur Card Systems.

For example, the "InspireD" project, which is receiving 9.2 million euros in funding from the European Union, seeks to create a standardized platform for all smart cards used across a range of "trusted personal devices", whether they are smart phones or television set-top boxes. The main idea is to make it easier for users to use their devices securely on the Internet. It may be to decrypt a broadcast of football highlights on a cell phone or make stock purchases on a PDA.

While other EU-funded smart card research projects have yielded few returns, this is the biggest of its kind, spanning three years and involving 16 organizations, mainly card and chip vendors, but also academic organizations. The participants are responsible for funding half the budget and see a need for the project to succeed, says Laurent Manteau, a manager in the research and development department for card vendor Gemplus, which is leading the consortium.

He expects the new smart card platform the consortium comes up with will look a lot like the new Java Card – it will support TCP/IP, be able to run multiple applications at the same time and break the bottleneck that now chokes communications between the smart card and other devices. In fact, it might

incorporate Java Card 3. “We are certainly quite successful in our market with the SIM card, with the banking cards,” says Manteau. “(But) we have certainly to evolve and to innovate.”

Before the InspireD group gets around to writing its final report, smart card vendors Axalto and Giesecke & Devrient say they will have introduced their own network smart cards, putting the TCP/IP stack onto the smart card along with replacing the smart card’s sluggish 7816 data-speed protocol with a speedy 12-megabit-per-second or higher USB interface. This turns the smart card into a node on the Internet, capable of interacting with thousands of existing and new Internet applications, says Axalto’s Montgomery.

The network smart card could support advanced versions of the secure sockets layer (SSL) of the Web while safe-guarding a cardholder’s payment data. Thus, the card could establish a secure link directly with the server of the Web merchant, just passing through the insecure PC. A user, for example, could buy tickets online then download them directly to the card, which he’d use at the theatre, perhaps with a wave of the card’s contactless interface, to gain entry to the performance.

We’ve heard this before. In fact, the network smart card may be one of the most hyped products in smart card history. Among its earliest appearances was at the Cartes expo in Paris in 1999, where former vendor Bull CP8 was touting the benefits of its “iSimplify” card. It planned to open competence centers on three continents just to develop all the applications that users and their Internet service providers would demand. Bull’s predictions that 250 million network smart cards would be in circulation worldwide by 2003 were premature, since few ever made it off the exposition floor.

Now, in these post-Internet bubble days, the projections are a little more sober, and this time the developers will soon have the technology to back up the hype.

This includes chips with enough RAM, at least 6K, to handle the TCP/IP stack and SSL security. These chips will also need the processing power to crunch the cryptographic algorithms associated with SSL, and they will also need to carry a full-speed USB interface to send data swiftly. The USB interface is probably the most important change. It eliminates the need for a card reader and middleware on the PC, as well as cranking up data speeds. All that would be needed is a connector linking the card to the terminal.

Some chips introduced in the past year deliver some of these attributes, but none have combined all three. “You’ll find multiple suppliers in 2005,” Montgomery predicts. That’s when both Axalto and G&D plan to move their network smart cards out of the demo booth and into the market.

“Any network application we use on a PC, we can now use with a smart card because it speaks the same language,” says Axalto senior engineer Asad Ali of the vendor’s “Web Identity Card.” ”It really opens the door to what we can do with a smart card.” For example, smart cards could handle security for the growing networks of sophisticated video games, and not just authenticating players to the service provider. The smart cards of two players facing off could talk directly to each other. “Then you wouldn't have a concern about cheating and the game data would reside on the card,” says Montgomery.

The changes, especially to such popular platforms as Java Card, poses risks to card vendors if they try to proceed too fast. The move could confuse customers, or cause them to hold off on purchasing high-end cards running the current platform while waiting for the new one. They may not believe vendor promises of backward

compatibility or that the vendors will continue to adequately support the old platforms.

But for the forward thinkers in the industry, failing to move smart cards to the next generation is not an option. "You can do that and die," says du Castel, Axalto's research director. "The smart card has to grow out of its limitations brought to it in the '80s."

Actual and projected Java Card shipments, in millions of units

Year	Units	% Growth
2002	165	
2003	220	33.3
2004	297	35
2005	398	34
2006	523	31.4
2007	680	30
2008	867	27.5

Source: Frost & Sullivan