MAKING NETSCAPE COMPATIBLE WITH FORTEZZA® – LESSONS LEARNED

George Ryan
gryan@pulseengineering.com
Pulse Engineering, Inc.
410-694-4900

ABSTRACT

This paper describes lessons learned during the development of Netscape products supporting FORTEZZA®, but many general principles are applicable to all commercial initiatives. All remarks in this paper express only the opinions of the author.

With the transition of Department of Defense (DOD) software products from Government Off-The-Shelf (GOTS) to Commercial Off-The-Shelf (COTS), changes are needed in the way security software is developed and evaluated. The government is undertaking an effort to develop applications to leverage emerging technologies and to broaden collaborative partnerships with industry, academia, and other government agencies to maximize the return from technology efforts.

KEYWORDS

FORTEZZA®, Netscape, security, World Wide Web, Secure Sockets Layer, Government Off-The-Shelf, Commercial Off-The-Shelf, Netscape Security Services

A. BACKGROUND OF NETSCAPE'S PRODUCTS USING FORTEZZA®

The United States government developed FORTEZZA®, an encryption system used by federal and government agencies, to manage sensitive but unclassified information. FORTEZZA® provides data security, integrity, originator authentication, non-repudiation, and confidentially. FORTEZZA® personalizes security through an individual cryptographic hardware device called a FORTEZZA® card.

Netscape provides a variety of web-based client and server software products. Netscape Navigator became the web-browsing client of choice during the early integration for FORTEZZA® by making a "special build" of Navigator to support FORTEZZA®. The "special build" is a modified version of the Navigator source code apart from the baseline product. Later, Netscape Communicator, which integrates email, groupware, editing, and browsing tools, replaced the client. Netscape Communicator has

a standard interface for cryptographic tokens that provides support for, among others, FORTEZZA®.

The servers that use FORTEZZA® are the Netscape Enterprise Server (web server), Netscape Messaging Server (mail server), Netscape Collabra Server (news server), and Netscape Directory Server. These four servers presently support FORTEZZA® as "special builds;" however, in the future, Netscape plans to incorporate the same standard interface for cryptographic tokens into these servers as they did for Communicator. There is an early FORTEZZA® version of the Proxy Server, which also supports FORTEZZA® as a "special build;" however, Netscape currently has no plans to incorporate a standard interface for cryptographic tokens in the Proxy Server.

Future versions of the base Netscape products will have no more "special builds" to specifically incorporate the FORTEZZA® functions. It will be integrated into the normal baseline commercial product in the future version 4.x clients and will be in 4.x servers. Because of scheduling conflicts, the current delivered 3.x products are still a separate product although they are supported as another Netscape commercial software product.

B. HISTORY

Incorporating FORTEZZA® into Netscape will be accomplished in three phases. The first two have been completed; the third is continuing today.

The purpose of the FORTEZZA® Phase One effort was to prove the concept that FORTEZZA® could be incorporated into Netscape in support of the Secure Sockets Layer (SSL) protocol. Support for FORTEZZA® is included in the SSL open protocol. Netscape products were designed to support the use of FORTEZZA® with SSL as an enhanced alternative to software-based cryptographic mechanisms. The client (Navigator 3.01) and server (Enterprise Server 2.01), as well as the Proxy server (Proxy Server 2.0), were FORTEZZA®-enabled as a "special build" of the software. This places the product in the hands of users, testers, and developers, giving all a feeling of what was needed to use Netscape with a hardware token. Although this release proved that FORTEZZA® could be incorporated with a major commercial software package, it was still a "special build" of the client and server. Phase One set the stage for Phase Two, which is incorporating FORTEZZA® into Netscape's other baseline products.

"Plug-ins" are software programs that extend the capabilities of Netscape clients and servers in a specific way, giving the user, for example, the ability to play audio samples or view movies from within Navigator. Phase Two incorporates FORTEZZA® "modules," which act as a plug-in, similar to other add-ons, to the basic Netscape "out-of-the-box" software [http://home.netscape.com/comprod/products/navigator/version_2.0/plugins/index.html].

The real test to see if Netscape follows open standards will be to determine whether non-Netscape products can be integrated with Netscape. The FORTEZZA®

plug-in is really an implemented Public-Key Cryptography Standard (PKCS) #11 interface to the FORTEZZA® hardware token. PKCS is a set of informal inter-vender standards developed in 1991 by RSA Data Security. PKCS #11 (Cryptoki) is a Cryptographic Token Interface Standard [http://www.rsa.com/rsalabs/pubs/PKCS/]. Most of the work in the first beta copy of Phase Two was re-coding the "special build" Phase One code to this standard. It is also important to note that as updates are made to the PKCS #11 standard, updates may also be necessary for the FORTEZZA® plug-in module.

Using standard cryptographic interfaces is consistent with the trend to commercialize the DOD applications. It takes advantage of Netscape's position as a leader in the web market because users are already familiar with the look and feel of Netscape's browser, which makes the learning curve easier. Because FORTEZZA® is to be supported as "just another algorithm," the path to future migration is open. The government can also take advantage of Netscape's "Mission Control" product to administer the software to a large number of users. After the initial release, all future FORTEZZA®-enabled products will be included with the baseline releases.

Not all of the Netscape Servers were FORTEZZA®-enabled during Phase Two. Netscape's Certificate Server was not FORTEZZA®-enabled because of the existing DOD Public Key Infrastructure (PKI). Originally, the government planned that all DOD-based users would use the existing high-assurance level (also know as class 4 certificate) PKI. However, with the accelerated trend from a high-assurance DOD PKI migrating in a commercial direction, an early commercial certificate server would have helped jump-start this process. More information on the DOD's PKI initiatives can be obtained from the "DOD Public Key Infrastructure Roadmap" document.

C. LESSONS LEARNED

A good understanding of the issues dealt with on the integration of Netscape and FORTEZZA® should help to facilitate future efforts on similar projects. These efforts should continue to increase and become beneficial to both government and industry.

C - 1. Rapid Turn-Around Time Needed

One problem with trying to commercialize a DOD effort is that the government is not accustomed to the rapid turn-around of beta products put out by industry. Typically, time (months or years) is needed to test, retest, and certify a product thoroughly before it is used. Normally, a product is tested and a 'pass or fail' indication is given. The government wants to thoroughly test a product before it's used and industry wants to take little time to test. Today, software products may be outdated by the time a formal test procedure is completed. With the rapid turnover of new software, test procedures will need to be written in a more general manner, or a more intuitive method of testing will be needed. Documentation for beta products is sketchy, so the tester needs to have a general

feel for how the software should work in finding application bugs. It is imperative to report bugs as soon as they are found so that correction can be made in the next update to the software. Also, the focus should be on separating problems unrelated to code evaluation, such as the configuration or other user and operating system errors, which would detract from fixing real Netscape application bugs. A big challenge of any commercial effort is keeping pace with the rapid and constantly changing information technology.

C - 2. Incentive Versus A Direct Contract

Because technology is changing so rapidly and because there is a general desire for less government control, the contract between the government and Netscape is different from many former contracts with other companies. It has no detailed specifications to follow or Critical Design Reviews to pass. In what is sometimes called an incentive contract, FORTEZZA® is to be implemented as "just another algorithm". The government will evaluate successive version of the product and suggest changes, but the general implementation is up to Netscape. The government will also buy licenses for commercial software rather than pay for specialized development. This will encourage a transition from government-funded GOTS products to commercially available COTS products.

Unfortunately, the priorities and expectations of government and industry do not always match. There are many good ideas by both government and industry, but there are limited amounts of time and manpower to make them happen. As a result, wanted features may not be implemented. Betas are often distributed quickly without documentation, and the user community at large is left to sort through what was done and to debug sparsely tested code. Future contracts need to be written carefully to insure that government and industry understand the expectations.

C - 3. Beta Testing

Commercialization gives the government a new job as a beta test site for Netscape software releases. A Beta Test Working Group (BTWG) distributes software and promotes the discussion of problems. Subcontractors Computer Sciences Corporation (CSC) and later Analytical Systems Engineering Corporation (ASEC) run test procedures and intuitive evaluation on beta releases.

In the process of making updates, testing, and re-testing, two of the biggest problems encountered were:

1. Version numbers of beta releases could not be easily obtained. Therefore, it was hard to ensure that testers were using the latest software. Because the FORTEZZA® program consists mainly of "special builds", configuration control was hard to maintain.

2. Migrations to new server and client versions were rough. Many settings needed to be configured manually as software was updated.

During testing, Netscape seemed to give a lower priority to FORTEZZA®-specific changes and bug fixes requested by the government to areas of the software that were not modular to all algorithms. Three examples of this were:

1. Providing automated Compromised Key List (CKL) updates and retrieval of archived CKLs;
2. Including access control and processing via security classifications;
3. Displaying a FORTEZZA®-specific padlock icon if the FORTEZZA® token was used.

Integrated test and evaluation is needed to assess the usability of commercial products for various environments.

C - 4. Netscape's "Expert Alliance" Support

Netscape Insight is a private extranet site exclusively for authorized Netscape partners. Users must possess a VeriSign Class 1 Digital Certificate to access the site. This site allows Netscape "partners" to have access to some of the information on Netscape's internal database [http://home.netscape.com/partners/programs/insight.html].

Keeping track of problems is a struggle when more than one tracking system is used. A Problem and Reporting Tracking System (PRATS) was developed for use by the government. A second tracking system - Netscape's internal CaseTracker Tracking System with simple HTML pages was also used during status meetings. Different testing organizations were reluctant to share their internal databases, and the official status of problems was often tightly guarded. Many prototypers are simply interested in getting something to work and will work around problems, rather than taking the time to document them. Informal Frequently Asked Questions (FAQ's), mail lists (the BTWG, and others), websites ([http://beta.missilab.com], [http://field.netscape.com/~ndug/index.html], and others), as well as Netscape's Newsgroups (news://secnews.newscape.com), have helped in disseminating information about problems and solutions.

C - 5. Interfacing With The Certificate Authority Workstation (CAW)

A high-assurance government CAW was used to integrate the DOD PKI with Netscape's commercial software. However, in the "medium-assurance level" (also know as class 3 certificates) commercial world, the rapid development of commercial PKI technology soon produced a PKI solution which, in some instances, seemed to be more functional than the government's DOD efforts. The DOD CAW only supports Version One X.509 certificates, while more commercial certificate servers, including Netscape, support Version Three X.509 certificates. Netscape's Certificate Server also could

generate and install certificates through the Internet, as opposed to sending a FORTEZZA® card to a specified location to be programmed. This is a considerable advantage in deploying a PKI solution in a timely manner. The price for a high-security PKI seems to be a slower production cycle.

C - 6. The Directory Interface

Interfacing to the Lightweight Directory Access Protocol (LDAP) standard helped integrate the DOD PKI design. A GOTS directory solution was already in place. After some incompatibility problems with earlier versions of LDAP, the LDAP client interface was successful in binding (connecting and searching) to the DOD and commercial directories, in addition to binding with Netscape's directory with anonymous binds. Incompatibilities such as the format and attribute location in the directory of Certificates, Comprised Key Lists (CKLs), and Certificate Renovation Lists (CRLs) make it a challenge to maintain support of applications that use directories. However, when applications can pull information from both commercial and government directories, an important step toward interoperation is accomplished.

C - 7. S/MIME With FORTEZZA®

An interesting issue came up in implementing Secure Multipurpose Internet Mail Extensions (S/MIME) version 2 with FORTEZZA®. Netscape used Version Three X.509 RSA certificates as defined in a S/MIME Certificate Internet-Draft. The government wanted to use the specification SDN.706 (X.509 Certificate and Certificate Revocation List Profiles and Certification Path Processing Rules for the Multilevel Information Systems Security Initiative (MISSI)) as the defining specification for FORTEZZA® [http://www.armadillo.huntsville.al.us/Fortezza_docs/index.html]. The Internet email address needs to be located in the certificate to be signed, but the two specifications have the Internet address in different places. SDN.706 could not be used with Version One X.509 MISSI certificates because it did not support the extension needed. In this case Netscape used the S/MIME Certificate Internet-Draft. The problem with this solution was that the government CAW could not support the Object ID (OID) needed to add the email address to the Distinguished Name (DN). As a result, S/MIME with FORTEZZA® never left the testing phase because there was no infrastructure support. This problem should disappear when the government CAW upgrades to Version Three X.509 MISSI certificates.

C - 8. Compromised Key Lists (CKLs)

A compromised key list is a file containing key information of all users with keys that have been comprised. This file must be continuously updated and distributed every few weeks to order for the Netscape software to allow a secure FORTEZZA®-enabled connection.

Several current customers tend to be dissatisfied with FORTEZZA® because of manual CKL file distribution mechanisms. Once the application was required to check the CKL, users became confused when they saw "invalid CKL" error messages. Typical users did not understand the meaning of these messages, they did not know how to get a new CKL, and their applications stopped working. The users with good network connectivity could, through a directory or web page, access their CKL. They tended to wait until they could no longer operate before updating the CKLs. They simply did not want to leave the work they were doing to perform an administrative function. If the only way to receive an updated CKL were through email, the problem shifted to reliance upon system administrators to distribute CKLs in a timely manner. Thus, the system administrator (which may also be the user himself) became a bottleneck for CKL distribution. A better solution would be to try to obtain network access for many or all of these users and provide for a Directory User Agent (DUA) or Web site solution for obtaining the CKL. CKLs also are not shared between applications. Therefore, a new CKL must be loaded for each FORTEZZA®-enabled application. When standard Cryptographic Applications Program Interface (CAPIs) are incorporated, such as Common Data Security Architecture (CDSA), a common Certificate Services Manager will correct this condition. A CKL is also a government-only solution; most commercial applications understand only CRLs, which are also used but frequently optional, in a GOTS solution.

C - 9. Software Libraries And Drivers

The government-funded effort to design FORTEZZA® libraries and drivers evolved to allow industry to take more of a lead in the direction of this technology. Drivers are responsible for getting data to and from the FORTEZZA® card, and libraries provide a higher-level interface for applications to communicate with the card.

Writing a PKCS #11 standard interface was one of the tasks Netscape accomplished in the Phase Two contract. Yet, this did not totally solve the problem of widespread interoperability with commercial Personal Computer Memory Card International Association (PCMCIA) readers. When an operating system or new technology evolves, any changes in the timing and hardware configuration require modification by the driver manufactures. The design of FORTEZZA® was frozen, yet updates to the PCMCIA standards, controller chip bug fixes, and other changes by industry were being made. This leads to the unfortunate situation in which users have a brand-new, state-of-the-art computer platform yet may not be able to use a card reader that works with FORTEZZA®. Drivers from the many supported platforms are continuously being updated as bug fixes and enhancements are made; they can be purchased from the venders. However, libraries and drivers provided by the government for no cost are presently frozen at their current revision.

Another issue arose when trying to integrate one FORTEZZA®-enabled Netscape application with another application that did not use the same drivers. Drivers from one

vender generally are not compatible with another vender's drivers. The long-term solution is for all applications to use an interface such as PKCS #11; however, many legacy applications were written before the PKCS standard. The problem is not unlike the attempt to maintain DOS compatibility when Microsoft Windows was developed.

C - 10. Card Readers

As mentioned above, using any generic card reader with a FORTEZZA® card was difficult because there were no mature standards for a PCMCIA card reader. Standards were rapidly being updated and changed as technology advanced. This is also a problem today in incorporating smart card readers into mainstream commercial products. Currently, smart card standards and specifications are being established (PC/SC Workgroup, PKCS #11, Open Card Framework, Java Card 2.0, etc.). FORTEZZA® cards were simply the first to encounter these problems before standards were developed, so there were no industrial trends to follow. Having interchangeable readers made by different card reader venders was not an easy task. Old card reader firmware (which can be updated by changing programmable gate array chips inside of the readers) and timing changes on new readers cause trouble on certain platforms with certain operating systems. The user can upgrade the firmware if the microcircuit is on a socket; otherwise, the reader (in some cases) is sent to the manufacturer and upgraded at the factory. With smart cards becoming more popular, better standards should help minimize these interoperability issues in the future.

C - 11. America-On–Line (AOL) Pop-Ups

Originally, individuals could not configure the core product (Communicator 4.04) to suppress the AOL instant messenger, even though Mission Control, with its broad application to multiple users, could do so. However, since individual users cannot use Mission Control the beta testers were troubled with these pop-ups. Having a commercial pop-up constantly appearing on a government computer is also awkward. Additionally, if a certain user or platform is always trying to access a non-standard port, it appears suspicious to system administrators when they routinely check firewall access logs for security purposes. Later versions of Communicator have a "Don't show this dialog again" checkbox at the bottom of the window, which will remedy the condition.

C - 12. Operating Systems

As newer versions of operating systems are adopted, venders will discontinue support of an older operating system. For example, Netscape no longer supports Solaris 2.4 and Windows 3.11. With the older operating systems, patches and Service Pack updates are needed before Netscape will run correctly. Recently, the newer versions of the FORTEZZA® servers have not always been guaranteed to support older operating systems, making the migration path from older versions of Netscape more difficult.

Despite cross-platform support, users cannot fall too far behind in keeping their operating systems up to date.

C - 13. Quality Feedback Agent

By default, a quality feedback agent is started whenever the Communicator client crashes. This is used to send information on the condition of the user's computer from the computer's memory back to Netscape via the Internet. This information is used to determine the reason for the crash [http://home.netscape.com/communicator/navigator/v4.5/qfs2.html]. Individual users can disable this function or it can be disabled through Mission Control; however, the burden is on the user or administrator to be aware of this and disable it if required for security purposes. Users with sensitive information on their computers need to be alert to any automated functions included in commercial software and take steps to protect their data, which also includes not indiscriminately entering data into a pop-up window.

D. PRESENT AND FUTURE SUPPORT WITH NETSCAPE SECURITY SERVICES (NSS)

With Phase Two, FORTEZZA® was successfully incorporated into Netscape's mainstream products. The next step was to customize and develop specialized interfaces into the core product for some of the many specific user groups. If the commercial application did not have sufficient security for a customer, a specialized add-on could be incorporated.

Phase Three, Netscape Security Services (NSS) set out to do so by developing a Netscape Security toolkit capable of interfacing with Netscape's internal certificate and key database. Tools were also provided to access the security database, including the PKCS interface. A Java and C interface to Netscape's data were both developed.

One example where the NSS could be used to help with a custom solution is in processing classifications between different FORTEZZA® cards by creating a server-side plug-in with the toolkit. Outside of DOD, though, there is presently not a widespread interest in such functions. The NSS functions as a toolkit, not as a Cryptographic Application Program Interface (CAPI).

D - 1. CDSA Support

CDSA is thought to be the long-range goal of the future by both Netscape and the government. CDSA is a set of programming interfaces that provide security services to applications. Because many venders helped to establish this specification and The Open Group endorses it, industry believes that CDSA will be the leading multi-platform security architecture followed by both government and industry. Unfortunately,

acceptance by industry in general has been slow, although, this may be changing in the future. At this time, Netscape and many other companies are not aggressively implementing this standard. There does not seem to be enough justification to rewrite existing working applications to follow this standard. The PKCS #11 interface is very similar to the Cryptographic Service Provider (CSP) interface of CDSA. All other potential CDSA interfaces that could have been used in the NSS seem to be implemented in a Netscape proprietary manner. The question now is whether the government should aggressively support CDSA or consider other possible alternatives such as PKCS #11, Java, or CryptoAPI.

D - 2. Software FORTEZZA®

Since a hardware high-assurance solution may be excessive in some areas, a remedy was sought to use the existing FORTEZZA® ciphers in a software-only solution. This helps alleviate some hassles in using card readers, drivers, and hardware tokens. The CAW would create an initialization file in a standard format, which would be used to create image (data) files. These image (data) files will be seen by an application as the equivalent of a hardware FORTEZZA® card. Netscape may support software FORTEZZA® only in certain applications; however, care must be taken to ensure that the government's PKI supports this as a viable option. A third-party vender may also support Software FORTEZZA® through the PKCS #11 interface. To be widely used, software FORTEZZA® will need to complete Federal Information Processing Standards (FIPS) FIPS-140-1 certification by the vender [http://csrc.nist.gov/cryptval/140-1/1401val.htm].

D - 3. Message Security Protocol (MSP), Partition Rule Based Access Control (PRBAC), And Other Security-Related Issues

Ideally, industry would support government-sponsored protocols. This would aid in a possible transition of software security products to COTS. MSP and PRBAC are examples of such protocols. Unfortunately, without a wide market for these specialized security solutions, it does not make good business sense to place a high priority on government-supported protocols, given the limited resources and investments that companies like Netscape are willing to put forward. Security labels and classifications may be able to solve problems with proprietary electronic communications in the future, but this is not something the commercial industry is currently requesting. The long-term solution seems to be the merging of commercial and government protocols. The Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3 proposed standard is an example solution, which can satisfy the needs of both government and industry. A freeware library is available [http://www.armadillo.huntsville.al.us/software/index.html].

E. DOD SITE-WIDE LICENSE

Many Netscape products are now covered under a site-wide DOD license. This arrangement should help to distribute Netscape's software throughout the DOD. The license includes both FORTEZZA® and non-FORTEZZA® versions of Communicator, Netscape Enterprise with LiveWire (Web) Server, Messaging (Mail) Server, Collabra (News) Server, Directory Server, Certificate Server, Mission Control (administrative functions), and Netscape Security Services (Toolkit). One advantage of this license is a move toward a common user interface independent of operating systems or platforms, which opens the door for future Java server and client-side applications. Also because of the modular nature of the Open Standards being implemented, there is the capability to include future algorithms and changes to existing algorithms. This "technical refresh" should allow future changes to be incorporated more easily without major changes to the user interface. This is particularly useful because the FORTEZZA® card is aging, and faster processors and more standards are evolving. An open interface standard leaves the door open for the FORTEZZA® card, a faster FORTEZZA® solution, or software FORTEZZA®. More information about the DOD license can be found on [http://www.menk.com/dod_license/].

F. CONCLUSION

FORTEZZA® can be used as a high-assurance GOTS solution (i.e., using the correct card readers, correcting versions of software with all patches, following established procedures, having the required training). It is a part of the Defense Messaging System (DMS), although much of the present work with FORTEZZA® is focused on email solutions. Government users will have to be more flexible about their requirements if we are truly to move toward COTS. In order to be supported commercially, FORTEZZA® needs to be user-friendly (plug and play), available, and desirable to use. Netscape integration with FORTEZZA® is a good start toward reaching these goals. It has uncovered and resolved a number of integration issues and has provided useful information for supporting future Netscape, FORTEZZA®, and other integration efforts. There also needs to be enough "hooks" into commercially funded software to allow modifications to accommodate users' needs. Support of CDSA or similar standards will help ease the transition of new products. Government funding of Netscape has encouraged other competing companies to also support FORTEZZA®, which would probably not have happened without this effort. Since FORTEZZA® is integrated into its products, it is desirable to have Netscape continue to maintain support for FORTEZZA® in the future. As with any commercial endeavor, market demand will probably determine whether or not this will be the case. Future directions will be increasingly interesting to follow as the AOL-Netscape merger progresses.

REFERENCES

1. FORTEZZA – [http://www.armadillo.huntsville.al.us/].

2. Netscape Products with FORTEZZA – [http://developer.netscape.com/tech/security/formsign/fortezza.html].
3. Government Programs - [http://www.nsa.gov:8080/programs/ncs21/goal4.html].
4. Government Documents- [http://www.cio.dla.mil/jgwi/docs/doclist.htm].
5. S/MIME – [http://www.armadillo.huntsville.al.us/software/index.html].
6. CDSA – [http://developer.intel.com/ial/security/specifications.htm].
7. X.509 – [http://www.nexor.com/info/directory.htm].
8. CRYPTOKI – [http://www.rsa.com/rsalabs/pubs/PKCS/].
9. The Open Group – [http://www.opengroup.org/].
10. FIPS-140-1 – [http://csrc.ncsl.nist.gov/fips/fips1401.htm].

National Information Systems Security Conference

MAKING NETSCAPE COMPATIBLE WITH FORTEZZA® – LESSONS LEARNED

George Ryan
gryan@pulseengineering.com
Pulse Engineering, Inc.
410-694-4900

PULSE ENGINEERING

Keeping Up with Technology

- **Old way**
  - **Solicit bids (RFP), award contract, Critical Design Review, test, report problems, retest, certify, deploy**
- **Leveraging emerging technologies**
  - **Rapid turnaround time of software applications**
    - **Technology doubling every 18 months**
  - **Economically better**
  - **Standards-based**
- **New way**
  - **Modify existing commercial design, beta test, evaluate, feedback, risk assessment, repeat process**
    - **Shorter learning curve**

PULSE ENGINEERING

History

- **Phase 1: Special Netscape "builds" to show "proof of concept"**
  - **FORTEZZA®-enabled web client, web server, proxy server**
  - **Special builds**
  - **1995**
- **Phase 2: FORTEZZA® integration as "just another algorithm"**
  - **FORTEZZA®-enabled web client, web server, directory server, news server, mail server**
  - **PKCS #11 modules**
  - **1996-1998**
- **Phase 3: Netscape Security Services (NSS) and Software FORTEZZA®**
  - **Security toolkit, Software FORTEZZA®**
  - **1998-1999**

PULSE ENGINEERING

Incentives for Support

- Contract written in general manner
  - FORTEZZA® as “just another algorithm”
- Seed money support
  - Hope that the vender will eventually support without funding
  - Encourage third party vender support
- Understanding needed between parties
  - Customer - guided away from proprietary solutions
  - Beta testing is important for key “features”
    - Return on investment (ROI) may not justify needed fix !!!
  - Future funding not guaranteed
    - Transition of people

PULSE ENGINEERING

Beta Site Testing

- Beta software of the past is today's final products
- Customer needs to debug
  - Independent testing needed
  - Continuing process
  - Maintenance support follow-on importance
- Sharing information from different testing groups
  - Beta Test Working Group (BTWG)
  - Mail lists to pass information - formal and informal
  - FAQ's
  - Informational web sites
  - Newsgroups - Netscape and government-sponsored

PULSE ENGINEERING

Software Configuration Control

- **Operating systems**
  - **Patches (Solaris 2.4), Service Pack updates, and hot fixes**
- **Drivers/ Libraries**
  - **GFE or vender-specific**
  - **Version numbers change with operating system**
- **Application build numbers (beta builds, Y2K patches)**
- **Administrative server updates with new Netscape servers**
- **Third party module revision numbers (PKCS #11 modules)**

PULSE ENGINEERING

Hardware Configuration Control

- **Card readers (FORTEZZA® now, Smartcards later)**
  - **Firmware version numbers (return for updates)**
  - **Serial numbers**
  - **ISA, SCSI, Parallel - now**
  - **USB, PCI - future**
- **Notebook computers - certified for NT?**
  - **Controller chips (different chips, same models)**
  - **BIOS updates**
  - **Standard updates (PKCS #11, S/MIME, LDAP, certificates, CRLs)**

PULSE ENGINEERING

Problem Tracking

- **Tracking Systems**
  - **Netscape**
  - **Independent tester**
  - **Government**
- **Long term support with personnel turnover**
  - **Bug fixes**
  - **Requests for enhancements**
- **Clear, detailed descriptions are important**
  - **All versions of devices and software**
  - **Repeatable months later**

PULSE ENGINEERING

Debugging Concerns

- High assurance security is not always the top concern
  - Ease of use and cost verses security
- Separate operating system problems from bugs
  - Test on different platforms
  - Install all patches
- Separate configuration problems from bugs
  - Test on several systems
  - Share information between testers
- Migration of FORTEZZA® servers
  - New generations of Netscape products
  - To other platforms

PULSE ENGINEERING

Other Concerns

- AOL Instant Messenger
  - Writes to non-standard ports
- Quality Feedback Agent
  - Computer's information sent back to Netscape for debugging
- Undocumented features (Ctl-Alt-F) - Fish Cam
- Only certain vender-specific brands of card readers
  - ISA, SCSI, Parallel, USB, PCI, Cardbus
- Multiple applications can only use one vender's driver at a time
  - Hardware conflicts over control of card

PULSE ENGINEERING

Examples of Desirable Features

- **CKL support (third party plug-ins may help)**
  - **Auto updates**
  - **CKL/CRL archiving**
- **Security classifications (third party plug-ins may help)**
- **FORTEZZA®-specific padlock**
- **Cryptographic API (CAPI) support**
  - **Faster/cheaper to continue proprietary solutions**
  - **Return on investment (ROI) not there**
  - **Little to test against for CDSA interoperability**
- **S/MIME version 3 support**
  - **Freeware library available**

PULSE ENGINEERING

PKI Support

- **Government infrastructure**
  - **Supporting both with government and commercial applications**
  - **High assurance PKI (FORTEZZA®) - security awareness**
  - **Medium assurance PKI (RSA) - commercial feasibility**
- **Minimum functionality or “proprietary extensions”**
  - **Version 1 verses version 3 certificates**
- **CRL/CKL support**
  - **Government - file distribution - web or directory**
  - **Commercial - going toward OCSP**
- **Ease of use**
  - **Programmed FORTEZZA® card versus web solution**

PULSE ENGINEERING

Directory Interface

- Storage place for certificates
  - Different OID's for government and commercial directories
- Non-standard formats affect posting and displaying
  - RFC 1778 - government CAW
  - Binary - Netscape Certificate Server
- Strong binds
  - DAP with FORTEZZA®- government CAW
  - LDAP over SSL- Netscape Certificate Server and client
- DAP and different versions of LDAP
- Web directory gateway verses Directory User Agent (DUA)

PULSE ENGINEERING

Netscape Security Services (NSS)

- **Lack of CDSA support**
  - **PKCS #11 interface verses CSP interface**
  - **Low ROI at this time**
- **Example programs with RSA only**
- **Software FORTEZZA® support**
- **How to test a Software Development Kit (SDK)**
  - **Several functions remain untested**
- **NSS functionality does not guarantee client/server functionality**
  - **PKCS #11 modules**

PULSE ENGINEERING

Conclusion

- More user-friendly “plug and play” FORTEZZA® solution desired
  - Installation and CKL/CRL updates
- Enforce standard-based solutions over proprietary solutions
- Continuous maintenance support needed
  - Recommend “hooks” into native software
  - Bug fixes
- Encourage market demand
  - DOD site license
  - Third party vender support
- Speak the language and sweat the details !!!

PULSE ENGINEERING