FOCAL POINT

Evaluator's Guide
A White Paper

Introduction

The benefits of Single Sign-On

The benefits of a Single Sign-On solution are well-known:

- Improved security, since users will not defeat the purpose of passwords by writing them down, posting them on their workstations, or using easy-to-guess strings such as the names of their pet.
- Reduced help desk costs, since fewer users will call for password resets or other password issues that eat up support time.
- Better productivity for users, since they will be able to access enterprise applications on any platform without needing to learn or remember how to logon to each one.

To realize these gains in your enterprise, however, you must carefully evaluate your options and select the solution that can truly deliver these benefits.

This *Evaluator's Guide* is intended to help you in that process.

Determining your requirements

To successfully deploy Single Sign-On today, most organizations have a set of key requirements that must be met. Here are some of the most common requirements expressed by organizations seeking Single Sign-On.

- You have a multitude of existing applications on multiple platforms—Windows, Web and legacy—that need to be integrated quickly into the Single Sign-On solution, with a minimum of effort.
- You need a highly available and scalable architecture.
- You need the lowest possible Total Cost of Ownership and the smallest possible IT management burden.
- You need a flexible authentication scheme that supports your choice of current and future technologies.
- You need a solution transparent to users that will not disrupt their daily routines.

This *Evaluator's Guide* describes how Focal Point meets all these requirements, and will help your enterprise gain all the benefits of a well-implemented Single-Sign On solution.

Quick Integration of Applications

To help evaluate competing Single Sign-On solutions, many IT departments challenge a short list of vendors to integrate a test set of applications. Using Focal Point's built-in tools, our consultants routinely succeed in integrating more applications in less time than any other vendor.

Why is it faster to integrate applications with Focal Point?

To start, Focal Point's design supports every major platform used by any modern enterprise. As well, Focal Point uses a more flexible set of integration tools, including an innovative set of software agents driven by XML parameter files that can handle most existing applications on any platform.

Multi-platform support

Focal Point supports every major platform used today.

The Focal Point client is designed for a heterogeneous network with workstations running any combination of Windows 95/98/ME/NT/2000/XP, Web browsers, Citrix, Linux, NCR UNIX and/or Solaris. The Focal Point server runs under Windows NT4 with Service Pack 5 or higher/Terminal Server/Windows 2000/XP/2003 or .NET.

The target applications for Single Sign-On can run on any platform accessible to the network including mainframes (OS/380, AS/400, Tandem and others), UNIX servers, Web servers, Windows NT/Terminal Server/2000/XP and .NET servers, Citrix, Novell NetWare, corporate databases, Lotus Domino and others.

Solid experience and support for all these environments ensures that your Single Sign-On system will be quickly rolled out to all your users, no matter what workstation and applications they need.

Flexible integration tools: agents and XML

As shown in Figure 1, Focal Point uses a flexible set of tools for integrating applications. At the highest level, a **Wizard** provides an easy-to-use GUI suitable for integrating common applications. The Wizard outputs one or more XML parameter files.

These **XML parameter files** provide a powerful and versatile mechanism for automating the logon process to any application. For more flexibility, these XML files can also be edited or hand-tuned using any standard XML editor or word processor.

The XML parameters are fed to one or more **software agents** to handle applications on specific platforms such as Win32, Web, terminal-based and on so. Additional agents are being developed to provide tight integration with other popular environments such as Java.

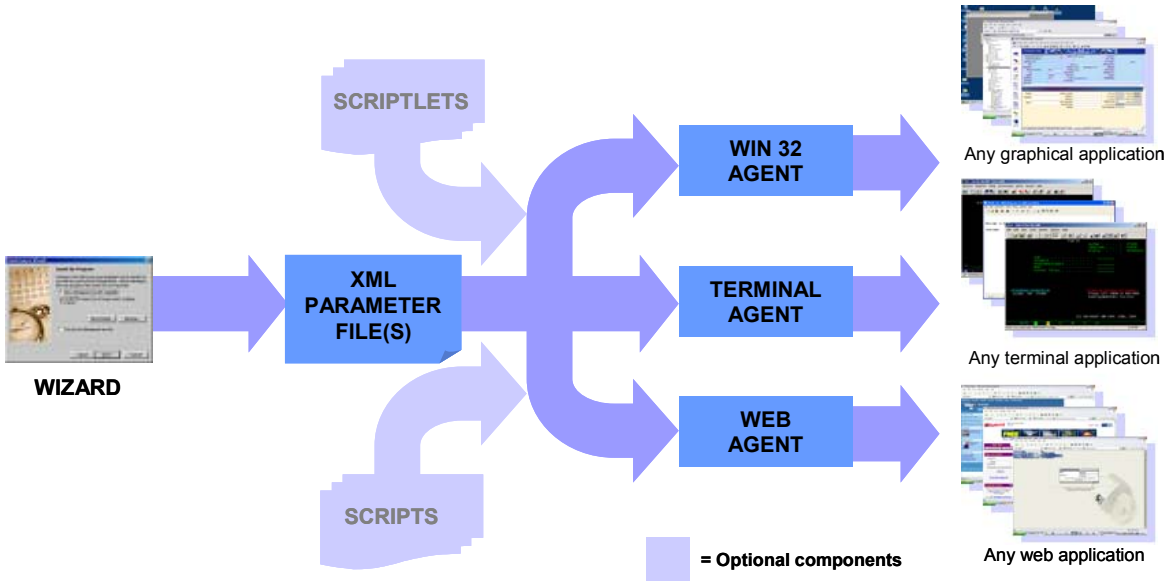

Figure 1: Focal Point Options for Integrating Applications

The **Win32 Agent** handles any application running under any 32-bit version of Windows including 95/98/ME/NT/2000 or XP. This agent uses the Win32 API to register in the Windows event loop. Whenever a relevant event occurs, such as opening a login or password dialog box or calling another application, the Win32 agent is triggered. The agent then loads the XML parameter file and takes the appropriate action.

The **Web Agent** handles any Web application accessed through any popular Web brow ser. The Web agent is launched as soon as the user starts a Web browser. This agent u ses the published APIs for these browsers to deal with any relevant event that can occur, such as opening another window for a different URL.

The **Terminal-Based Agent** handles any application running through terminal emulators including any 3270 or 5250 emulator with an EHLLAPI interface. It also supports any Telnet or X-Windows emulator with an automation API, such as Attachmate Extra, Hummingbird Exceed, WRQ Reflection and others, that can give this agent access to the screen and notify it whenever a relevant event occurs or the presentation space changes. This covers virtually all IBM, Tandem, Unisys and UNIX platforms running your enterprise or legacy applications.

Depending on your requirements, you can use any or all agents to automate the logon process for your applications. These agents are DLLs written in C++ that reside (along with the corresponding XML files) on every workstation in the Single Sign-On network. Since these agents are event-driven DLLs called only when needed, there is no ongoing process stealing CPU cycles and no performance degradation.

Handling special conditions with scriptlets

In a small number of cases, the application behavior may be so complex that a parameter file alone cannot handle it. These cases can be handled with **scriptlets** (short segments of script code). An agent can launch a scriptlet at any time when it encounters a condition it cannot process.

Each scriptlet defines simple "rules" for handling tasks such as decoding a string in a URL, launching another program and pushing a button, and so on. If you need to write a scriptlet, you can use any scripting language of your choice including JavaScript, perl, Tcl/Tk, Visual Basic or VB Script.

The last resort: writing scripts

Focal Point provides a fully documented API. At the lowest level, complete **scripts**, DLLs or executables can be written to call this API and automate the logon procedure for an application. This can be the most effective way to handle certain cases such as a legacy application for which no source code is available. These programs can be written in any language of your choice including C, C++, Java or Tcl/Tk.

(If source code is available, you can integrate an application by tweaking its code to call the Focal Point API with no need for any scripting.)

Why not just write a script for each application you need to integrate? In fact, some Single Sign-On solutions use this approach. As you can imagine, this is a much slower method that involves writing and debugging lengthy amounts of code. Our experience has shown that writing, testing and debugging an XML file to integrate one application typically requires 2 hours or less. Writing the equivalent Tcl/Tk code to accomplish the same task typically requires up to 2 full days. Scripts are a last resort when no other method will do.

As a third-generation Single Sign-On solution, Focal Point uses powerful software agents and XML parameter files to provide much quicker integration of the vast majority of applications. Writing programs is reserved for the exceptional cases that cannot be handled in a more efficient way.

The logic of integration

The Focal Point XML parameter files are based on viewing any well-behaved application as a finite-state machine with a defined set of states, conditions, and input and output events. Every foreseeable state, field entry, dialog box, URL and special case are identified in advance. This includes every possible password state: wrong credentials, expired password, multiple logons, and so on. With the corresponding logic engine built into the agent, Focal Point provides a very robust integration platform.

Creating XML parameter files

The parameter files used by Focal Point are compact, easy-to-read text files written in industry-standard XML. The completely open nature of XML means you are never locked into any one vendor or tool. Focal Point is bundled with documentation, sample files and tools to help your IT staff quickly learn how to create these files.

Working from an existing XML file, the first application may take your IT staff an hour or two to integrate. The next may be only a few minutes.Our consultants can work with your IT team however you prefer. We can create the XML files for you, or train your staff to write them, or work with your team to quickly integrate applications while they learn the process. From then on, your IT staff will be completely autonomous and able to integrate and maintain any future applications that you require.

Easy to read, easy to write

Figure 2 shows a code sample from a Focal Point XML parameter file. Anyone familiar with HTML will recognize the syntax of opened and closed tags.

The `<state>` tag defines a unique state such as logon, password change or verification. Here `<state name="init">` means the application's initial state. `<window>` defines a window so the agent recognizes it when it opens. And `<window text="Login">` refers to the window called "Login". (Since many applications feature windows with identical titles, Focal Point links each window to its appropriate executable.)

The `<control>` tag defines a control in a window such as a button, text box, field and so on. Here `<control class="Edit" index="0">` refers to the first text box and `index="1"` to the second text box, while `class="Button" text="OK"` refers to the pushbutton labeled "OK".

The `<action>` tag defines what action to perform on the selected control. Here `action type="settext"` means fill in the text field with the given variable. So the first two actions fill in the User ID and Password fields with the appropriate strings stored by Focal Point. Then the final action clicks the OK pushbutton. Easy to read, and easy to write!

Figure 2: Sample from XML Parameter File

```
<state name="init">
   <window text="Login">
        <control class="Edit" index="0">
            <action type="settext" fpname="LogonUserId"/>
        </control>
        <control class="Edit" index="1">
            <action type="settext" fpname="LogonUserPwd"/>
        </control>
        <control class="Button" text="OK">
            <action type="pushbutton"/>
        </control>
        <transition state="verification"/>
    </window>
</state>
```

Highly Available, Scalable Architecture

The Internet has conclusively proved the benefits of a decentralized network.

Designed to withstand nuclear attacks during the Cold War, it has been resilient in the face of more recent threats such as self-replicating worms and Denial of Service attacks. While service sometimes slows when the network is overloaded by malicious traffic, the Internet is never completely "shut down."

Like the Internet, Focal Point relies on a highly decentralized client/server architecture This architecture can deal gracefully with the temporary unavailability or loss of many network resources, yet still remain in service.

What makes this approach so resilient? Focal Point uses a simple but effective scheme of assigning multiple servers per client, which provides a highly fault-tolerant network that can be balanced and scaled up in a straightforward manner.

Multiple servers per client

Focal Point's architecture parallels the distributed nature of most modern enterprises. During installation, a list of Focal Point servers is assigned to each client workstation. If any client cannot connect for any reason to its first assigned server, it automatically switches to the next server on its list. This process continues until the unlikely event that the entire list of servers is exhausted without finding a single working server.

This design makes the network quite tolerant of faults and keeps Focal Point highly available with no added IT management effort. It also streamlines network maintenance, since any server can be upgraded, patched, reconfigured and rebooted with no impact on the Single Sign-On operations.

Isn't UNIX more reliable?

Many IT managers consider UNIX inherently more reliable than Windows. This may be true for applications where you can simply compare uptimes between a single Windows server and a single UNIX server.

But by using a number of Windows servers arrayed in a fault-tolerant design, Focal Point greatly boosts the effective reliability of Windows. With multiple servers and replicated databases of user credentials, it provides built-in redundancy for 24/7 availability. This has enabled Focal Point to achieve availability figures typically associated with mainframes and much more expensive UNIX platforms.

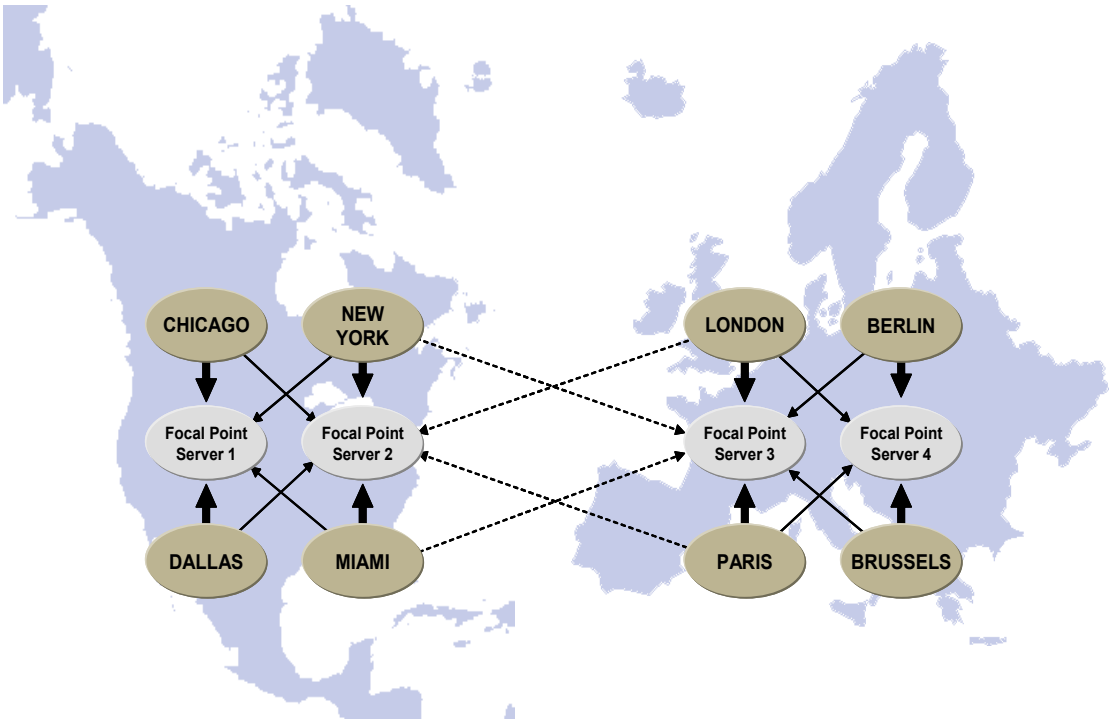

Figure 3: Focal Point Server Connections for ACME Enterprises

The network for ACME Enterprises

Consider ACME Enterprises, an operation with eight sites across North America and Europe supported by four Focal Point servers, FP1 through FP4. As in most organizations, these servers are located close to the largest concentrations of users. Figure 3 shows the primary server connections for each site; in other words, the default machines called by every workstation for Single Sign-On services.

If any primary server times out for any reason, the Focal Point client simply switches to its secondary server, shown by the darker lines in Figure 4, and continues to operate. While these diagrams show only two sets of server connections, in reality each client workstation is typically assigned a longer list that includes multiple servers.

Built-in scalability

Focal Point was designed from the start to support the very high number of users that some organizations may require. This Single Sign-On network is inherently scalable for a number of reasons:

- The server software makes efficient use of existing hardware.
- Each server can support a large numbe of Focal Point users.
- Additional servers are straightforward to add.

For example, if your organization already has a number of domain controllers, you may be able to deploy some or all of the Focal Point servers on your existing hardware. You may be able to run Focal Point and Active Directory on the same hardware. These are just two examples that show how Focal Point has been designed for scalability.

To rebalance the network, the network administrator can perform a load model calculation and reallocate certain users to different servers at any time. In this way, Focal Point provides a flexible strategy to optimize network traffic between clients and servers. Such a decentralized network is unlikely to hit any bottlenecks.

An effective track record

The technology behind Focal Point has been in daily use for more than a decade in large banks and financial institutions, private enterprises and government departments. Many thousands of users in these organizations rely on this solution for daily access to their mission-critical business applications. Extremely high availability has been measured in the field, with clients enjoying years of uninterrupted service from their Focal Point systems.

Low Total Cost of Ownership

Focal Point is perhaps the most cost-effective Single Sign-On solution in the industry.

It provides effective strategies for leveraging your existing system resources and IT personnel. It integrates smoothly with your current infrastructure. And it runs on a low-cost Windows/intel hardware platform. This all adds up to a very low Total Cost of Ownership that makes for a quick return on your investment.

Leveraging existing resources

With Focal Point, you can leverage your existing system resources instead of reinventing the wheel.

You can access your existing user, group and workstation definitions from wherever they are currently stored. In most cases, Focal Point can simply access an existing LDAP-compliant enterprise directory such as Active Directory, iPlanet Directory Server or Novell eDirectory. Otherwise, you can import user credentials from any ODBC database. This flexible strategy for reusing the existing user definitions eliminates the single largest cost in any Single Sign-On implementation.

From then on, users are simply added, modified and removed from the primary security domain to which Focal Point has instant access. There are no further user management tasks required.

Leveraging existing IT personnel

Our consultants can team up with your staff to leverage their existing knowledge and skills. We can perform the application integration for you, or do it with you, or train and support you to do it yourself. We will transfer our knowledge through detailed documentation, sample libraries and utilities to help your staff quickly become proficient at integrating applications and supporting your Single Sign-On solution. Our engineers can remain on site during any critical phase of your project. In short, we will work with your people as you prefer to get the best results from your implementation.

Smooth integration

Focal Point is designed to fit smoothly into your existing infrastructure. You can deploy it without any impact on your existing back-end systems or Web applications. You can maintain your existing replication and backup strategies without change. Users can download and populate their Focal Point clients themselves, or you can use your normal software distribution system such as CA-Unicenter, Microsoft SMS, Tivoli or any other tool. If you have a strategy to Web-enable your legacy applications, you can simply extend the Single Sign-On solution to each further application as it comes online.

Cost-effective hardware platform

One cornerstone of Focal Point's design philosophy has always been to provide a highly cost-effective hardware platform. Although our designers know and appreciate UNIX very much, in this instance selecting Windows is much less costly. This is why the Focal Point servers are designed to run on Windows/intel hardware with the load distributed across a number of easy-to-afford, easy-to-replace machines.

Numerous global vendors such as Dell, HP and IBM are continuously lowering the price points and increasing the power of this platform. Focal Point was designed to take advantage of the reality of Moore's Law and deliver its benefits to clients in the form of an extremely cost-effective server platform. By designing around the limitations of each individual Windows/intel box, we boost this platform's reliability while retaining its cost-effectiveness. This gives Focal Point the best of both worlds.

Few people in the IT industry would argue that it is more costly to source Windows/intel machines than the equivalent UNIX platforms. We invite you to do your own math and test this claim. We believe you will arrive at the same conclusion: that Focal Point provides a highly cost-effective hardware platform.

Flexible Authentication Scheme

Focal Point provides a completely flexible authentication scheme that preserves your investment in existing technologies and supports your choice of any future technologies.

Figure 5 shows how Focal Point sits "beneath" whatever authentication scheme you choose, both now and in the future. You can select whatever technologies you prefer today, including any combination of PKI, biometrics, smart cards, USB tokens, PINs and passwords. And you have a clear migration path to any technologies that are still on the drawing board. Focal Point supports them all.

And Focal Point provides this flexible support without replacing the critical Windows file, MSGINA.DLL (Microsoft Graphical Identification and Authentication DLL), which governs the primary authentication logon. Replacing this DDL, as some competing solutions do, is a risky business that can create numerous technical difficulties.

Implementing Focal Point is done as a separate project from enhancing your authentication methods. Then if you decide to reinforce your authentication methods at some point in the future, this means that you automatically reinforce your Single Sign-On solution as well.

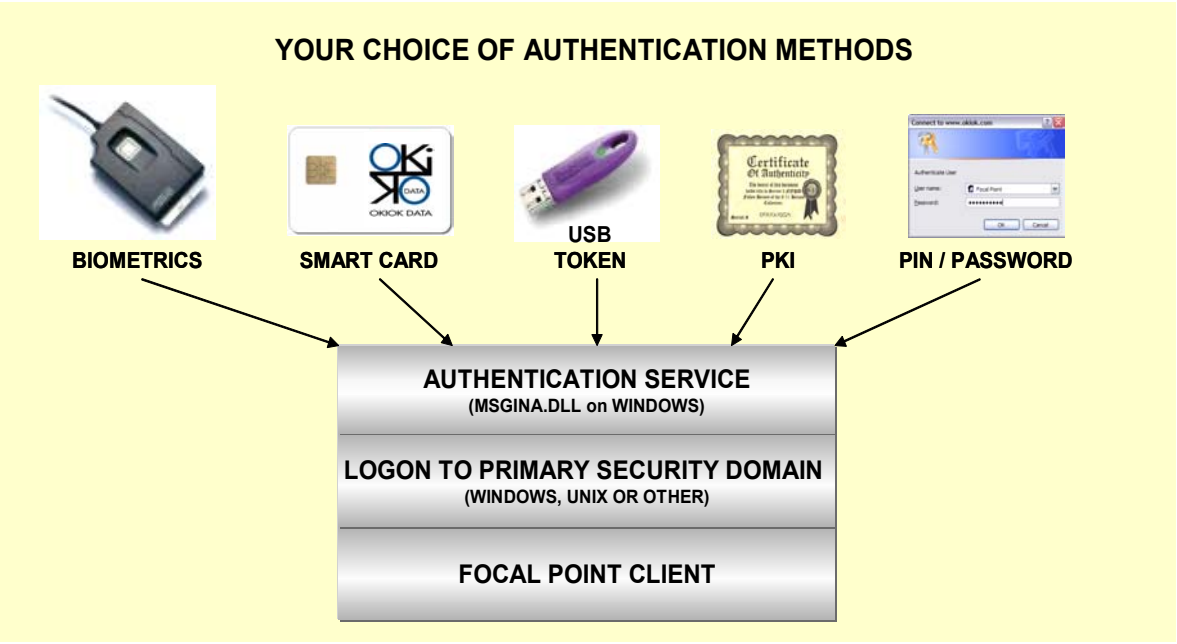

Figure 4: Current and Future Authentication Technologies

Transparent to Users

Some new systems hold out wonderful promise but are decidedly painful to implement.

One prominent business magazine called implementing an Enterprise Resource Planning (ERP) system, for example, "the corporate equivalent of a root canal." Not so Focal Point, which is completely transparent and painless to your users.

With Focal Point, users log on to the Windows network and launch all their applications by clicking an icon or selecting from the Start menu the sams as always. Unlike competing solutions, the Focal Point installation does not remove or replace any icons on the desktop. This means no learning curve and no disruption to the normal routine.

Alert users may notice that the Win32 agent shows in their Windows System Tray. After their first logon of the day, users will notice that the signon screens for each further application are displayed and populated automatically by Focal Point with no intervention on their part. In fact, they have less to do and less to remember.

This automated logon saves a small amount of time over manually entering and re-entering credentials. That leaves your users free to focus more on their mission-critical tasks. Multipled across thousands of users and a dozen applications, this somewhat enhances productivity.

With no learning curve, no training requirements, and no change to the daily routine, Focal Point is completely transparent to users.

Conclusions

This *Evaluator's Guid*e has shown how the Focal Point Single Sign-On solution meets all the key requirements of today's organizations, including:

- Quick integration of the vast majority of existing applications—Windows, Web and legacy—through powerful agents and XML parameter files. Scripting to handle exceptional cases is available in the language of your choice.
- A highly available architecture based on multiple servers that provide fail-safe operations that can scale up to support thousands of users.
- The lowest Total Cost of Ownership achieved through leveraging your existing resources and adopting a cost-effective Windows/intel server platform.
- A flexible authentication scheme that preserves your investment in existing technologies and supports your choice of any future technologies.
- Transparent operations that require no learning curve, no training and no disruption to the normal working routine for your users.

About OKIOK Data

Our mission

OKIOK's mission is to define, develop and bring to market enterprise security solutions that address the fundamental issues in today's evolving technological landscape.

Our flexible solutions are designed to help enterprises both leverage their investment in legacy systems and harness the full power of emerging technologies.

Our history

OKIOK has been at the forefront of the Information Security field since 1983. As such, we pioneered several key security concepts at the heart of modern IT security, including transparent disc encryption and Single Sign-On.

These concepts found their way into the various security solutions and product families developed by OKIOK to meet the requirements of government, banks and industry.

Since 1992, we have provided consulting service focused exclusively on IT Security. We have worked with numerous public and private sector clients in various roles, from cryptographic specialists to high-level advisors on corporate security.

Our highly skilled personnel include senior engineers, software developers, hardware designers, network security specialists, cryptologists and technical project managers.

We draw upon many years of secure product design, implementation and deployment as well as active participation in several standards committees including ANSI X9E9, CAC/ISO/IEC/SC27 and SSE-CMM PMACS.

How to contact us

Web: **www.okiok.com**

Telephone: **450-681-1681**

Fax: **450-681-1682**

Email: **info@okiok.com**

Mail: OKIOK Data, 3945 St-Martin West, Laval, QC H7T 1B7 Canada