White Paper:

M-Pin™

Multi-Factor Authentication Platform

Version: **1.4**
Updated: **29/10/13**

Contents:

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

M-Pin is a multi-factor authentication platform based upon the M-Pin Protocol, a zero-knowledge proof authentication design. The M-Pin protocol was developed by CertiVox from the initial research and publication of Dr. Michael Scott in 2002 into elliptic curve bilinear pairing cryptography, and updated in a new cryptographic research paper also available on the CertiVox Labs website.

Dr. Scott is the Chief Cryptographer at CertiVox, and the head of the CertiVox Labs research team in Dublin, Ireland. The M-Pin protocol has been extensively peer reviewed over the last decade, and no known practical flaws or attacks against it are presently known.

The M-Pin Multi-Factor Authentication Platform removes the password as an authentication mechanism entirely. In its place is the M-Pin Authentication Server, which uses the M-Pin Protocol for identity verification. Leveraging the properties of zero knowledge proof constructs, the M-Pin Server has just one leak-proof cryptographic key. If the server key is compromised or stolen, it cannot reveal information about user identities, or the credentials they use to authenticate themselves, to an attacker.

In addition, M-Pin improves the authentication user experience. The M-Pin authentication client is just an HTML5 browser; no browser plugins are required. Where a user would normally see a username password input field on a website, the user interacts with the M-Pin Pin Pad, an ATM style pin pad. The M-Pin client uses the OpenID Connect Account Selector paradigm, where the identities of the account can be selected, so the user only needs to remember their 4-digit pin. This is an infinitely better user experience than a username password or other two-factor authentication products.

Finally, M-Pin provides strong two-factor authentication using just a browser, enabling real 'something you have' and 'something you know' authentication, based upon strong elliptic curve cryptography. M-Pin can even be extended to include multiple factors, like biometrics and location.

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

About multi-factor authentication

Multi-factor (i.e., two or more factors) authentication is now a requirement across a range of industries ranging from financial services, to healthcare and government sectors.

As an example, in the USA, the Federal Financial Institutions Examination Council's (FFIEC) issued guidance for financial institutions that recommends implementing security measures to reliably authenticate customers remotely accessing their Internet-based financial services. The FFIEC identified three authentication factors as:

Multi-factor authentication is commonly defined as:

- Something the user knows (e.g. password, PIN);
- Something the user has (e.g. ATM card, smart card); and
- Something the user is (e.g. biometric characteristic, such as a fingerprint)

These guidelines recommended the use of "authentication methods that depend on more than one" of these three factors (i.e. "multi-factor" authentication). Note, many vendors have attempted to define multi-factor authentication as utilizing "other factors" such as the user's behavior; however, those methods are not approved by the FFIEC.

Following the above publication, numerous authentication vendors began improperly promoting challenge-questions, secret images, and other knowledge-based methods as "multi-factor" authentication. Due to the resulting confusion and widespread adoption of such methods, on August 15, 2006, the FFIEC published supplemental guidelines clarifying that such methods do NOT constitute multi-factor authentication:

"By definition true multi-factor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multi-factor authentication."

Multi-factor authentication is not a new concept, having been used throughout history. As an example, when a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card the customer slides into the machine ("something the user has"). The second factor is the PIN they enter ("something the user knows"). Without both of these factors, authentication cannot succeed. This scenario illustrates the basic concept of most two-factor authentication systems; the "something you have" + "something you know" concept.

About zero knowledge proof authentication protocols:

A zero knowledge proof protocol is a method by which one party (the prover) can prove to another party

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

(the verifier) that a given statement is true, without conveying any additional information apart from the fact that the statement is indeed true. For cases where the ability to prove the statement requires some secret information on the part of the prover, the definition implies that the verifier will not be able to prove the statement to anyone else. Notice that the notion only applies if the statement is being proven via the fact that the prover has such knowledge (otherwise, the statement would not be proved in zero-knowledge, since at the end of the protocol the verifier would gain the additional information that the prover has knowledge of the required secret information).

This is a particular case known as zero-knowledge proof of knowledge, and it nicely illustrates the essence of the notion of zero-knowledge proofs: proving that one possesses a certain knowledge is in most cases trivial if one is allowed to simply reveal that knowledge; the challenge is proving that one has such knowledge without revealing it or without revealing anything else.

For zero-knowledge proofs of knowledge, the protocol must necessarily require interactive input from the verifier, usually in the form of a challenge or challenges such that the responses from the prover will convince the verifier if and only if the statement is true (i.e. if the prover does have the claimed knowledge). This is clearly the case, since otherwise the verifier could record the execution of the protocol and prove it to someone else, thereby contradicting the fact that proving the statement requires knowledge of some secret on the part of the prover.

About Pairing-Based Cryptography (PBC)

M-Pin exploits the rapidly maturing science of pairing-based cryptography (PBC). Pairing-Based Cryptography provides an extra structure, which often allows solutions to complex problems that proved intractable to the standard mathematics of Public-Key Cryptography.

The poster child use case for PBC was Identity-Based Encryption, whereby the identity of a client became their public key. The idea was around for a long time, but traditional cryptographic primitives failed to produce a solution. However with the introduction of PBC, solutions were found almost immediately.

Putting it all together

M-Pin inherently includes techniques that support a multi-factor authentication, by exploiting PBC, whereby the user authenticates via a cryptographically strong secret, associated with their identity, and issued by a Trusted Authority (TA). The uniqueness of the protocol comes through the employment of the secret in a zero knowledge proof protocol, as the secret is divided between a conceptual physical (or “virtual”) token and a memorized PIN number, and (optionally) a biometric or other measurement, providing true multi-factor authentication.

Put in simple terms: M-Pin running in a standalone mode delivers true two-factor authentication using nothing more than your HTML5 browser. Coupled with additional factors, it becomes a multi-factor

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

solution. M-Pin achieves this with no additional client software or hardware required.

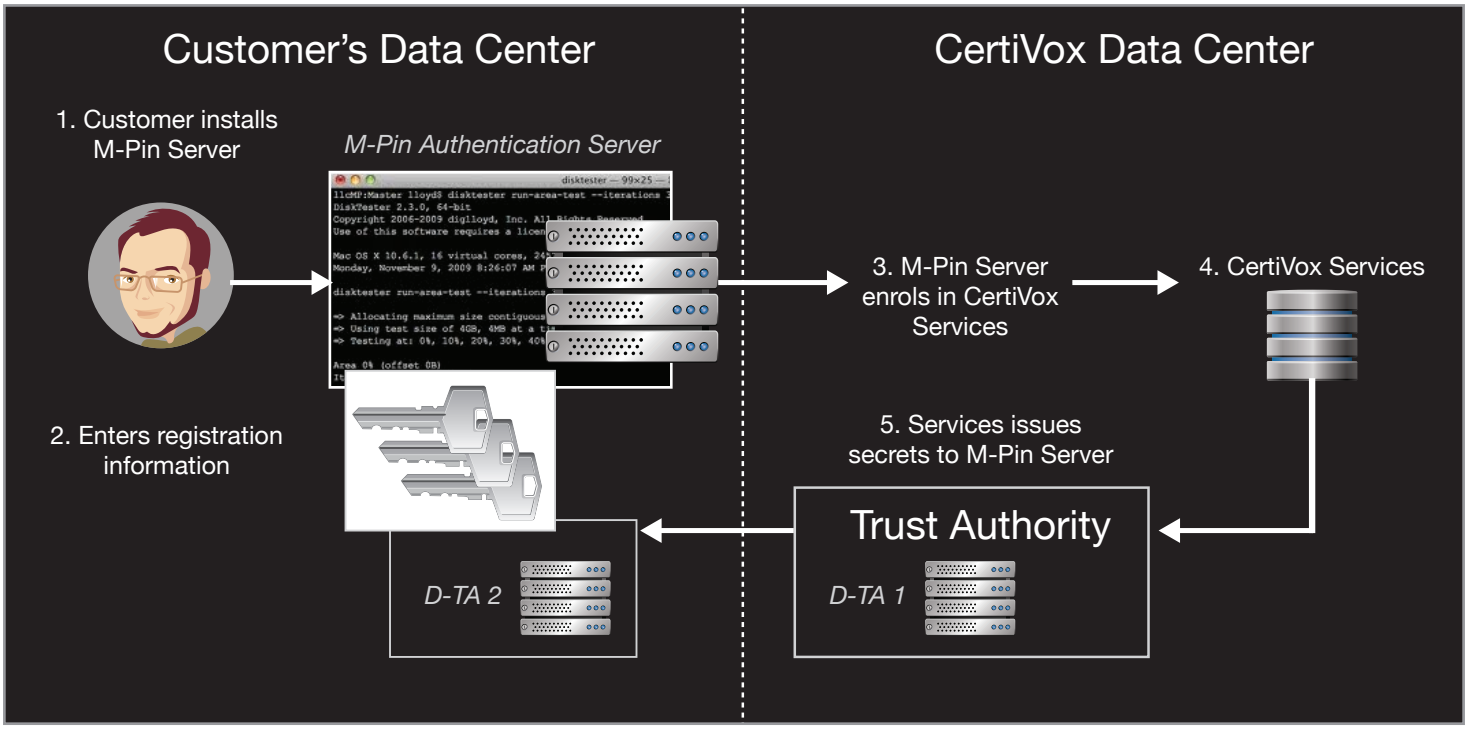
The M-Pin Authentication Server is not required to store any information derived from the user's secrets or PINs, so there is no equivalent of a vulnerable "password file" stored on the M-Pin Server. In fact, neither the PIN nor a biometric should be stored anywhere (other than in the user's memory or as part of the user's body respectively).

Lastly, because the solution is built on top of the MIRACL library and benefits from CertiVox's expertise of building protocols for low powered or constrained environments, the M-Pin client is run on browsers directly, including mobile device browsers as HTML5 web apps. For an in-depth cryptographic analysis of the M-Pin protocol, please visit the CertiVox Labs website at certivox.com to download the research paper, "M-Pin Technology."

M-Pin in your environment

The M-Pin Platform employs the concept of Distributed Trusted Authorities (D-TA) nodes. One D-TA node, run by CertiVox, generates one half of a master secret and then issues half of the identity-based secret keys to servers and clients utilizing the M-Pin Platform. The M-Pin Server, run by CertiVox customers in their environments, operates another D-TA node and independently generates the other half of the master secret. This 'on-site' D-TA node issues the other half of the identity-based secret keys to servers and clients utilizing the M-Pin Platform.

Clients use their email address as the unique identifier. M-Pin Servers use a randomly generated GUID as their unique ID. Using identity based elliptic curve cryptography, the ASCII strings and GUIDs are



T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

hashed to a point on the elliptic curve to produce each client and server's identity-based secret (a numerical string); again, for a client, this is representing his or her identity on the system by way of an email address. When the user registers their identity, it is the D-TA nodes that provide them with the halves of their cryptographic secret, not the M-Pin authentication server.

During the initialization process, the user's half-secrets are sent over HTTPS to the user's browser. The user is asked to initialize the combined, whole, cryptographic secret into an "M-Pin token" by entering their 4-digit pin via the M-Pin pin pad JavaScript application, also served down over HTTPS, with the domain secured by DNSSEC to prevent cache poisoning. Note that only the user will know her 4-digit PIN, as the pin pad runs locally, and sends no communication about the pin pad to the M-Pin service.

By selecting a 4-digit PIN, the M-Pin pin pad JavaScript application initializes the user's cryptographic secret into a "token", one that can be stored insecurely. Why? Without the 4-digit pin, it's impossible to re-assemble the strong secret. Utilizing the capabilities of HTML5 browsers and their ability to lock stored data objects to domains, the M-Pin pin pad JavaScript application stores the "token" in the HTML5 browser's storage area "locking" the token to the domain of the M-Pin pin pad JavaScript application. Again, picture this as analogous to writing a number onto a magnetic stripe of an ATM debit card.

When the user attempts to authenticate to an M-Pin Server, the M-Pin pin pad is served to the user's browser over HTTPS. In the following description of the operation, you can think of the M-Pin pin pad as analogous to the pin pad on an ATM terminal, authenticating the holder of a debit card when the debit card is inserted into the ATM machine. A mathematical process utilizes the information on the magnetic stripe of the ATM debit card (something you have), and the user's 4 digit PIN (something you know) to create the correct credentials to authenticate the user and enable them to access their account.

In order for the user to authenticate to the M-Pin service, the user enters their 4-digit PIN into the pin pad that is now running locally on the user's machine, inside of their browser. Since this pin pad was served from the same M-Pin service domain that originally served up the user's strong secret and then stored it in the user's browser database storage, (after being initialized with the user's PIN), only the M-Pin Server's service domain can access the "token" stored in the user's browser with the M-Pin pin pad JavaScript application, running locally. When the M-Pin pin pad is served up again to authenticate the user, the pin pad, running locally on the user's machine, accesses the user's token in their browser's storage, accepts as input the user's 4-digit PIN, and reassembles their strong secret from the combination of the "token" and the 4-digit PIN.

As described previously, once the M-Pin pin pad reassembles the user's secret, it is ready to be used in the zero-knowledge proof authentication protocol. ***Note that this is not presenting the user's secret to the authentication service as a password.***

Instead, the user's secret is used as a cryptographic parameter inside of the M-Pin zero knowledge proof

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

protocol, itself an underlying elliptic curve bilinear pairing cryptosystem. The detailed cryptographic paper is available on the CertiVox Labs website which illustrates its construction; "M-Pin Technology."

M-Pin Security

Before M-Pin™

Username/Password authentication

- Difficult to remember
  Insecure – easy to phish, scam, key log, etc.
- Bad user experience leads to insecurity

Username/Password database

Username	Password	Email
Bob28	sarah	Bob28@hotmail.com
v.Noir	password123	Vince.noir@yahoo.com
Alice_467	linkedin	Alice.h@gmail.com
Sarah.h!	facebook1	S.hard@gmail.com
Samsam10	hello	Sam@yahoo.com
sunnykid1	Pass1!	sunny@mail.com

- Databases are inherently not secured and difficult to protect
- "Smash and Grab" attacks are the new normal
- Liable for legal action if hacked

After M-Pin™

Multi-Factor Authentication

- 4 digit PIN - infinitely easier than username / password
- Elliptic curve crypto is infinitely more secure than username / password

M-Pin Authentication Server

Username	Password	Email
Bob28	sarah	Bob28@hotmail.com
v.Noir	pass[illegible]123	Vince.noir@yahoo.com
Alice_467	linkedin	Alice.h@gmail.com
Sarah.h!	facebook1	S.hard@gmail.com
Samsam10	hello	Sam@yahoo.com
sunnykid1	Pass1!	sunny@mail.com

- With M-Pin there is no username / password DB, just one server crypto key
- If the key is compromised, it reveals nothing about the users on the system

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

One of the obvious questions is the security of the token itself. M-Pin Tokens leak no information about the actual identity based secret issued from the TA to the client once they have been initialized with the 4-digit PIN. This is important to avoid “off-line dictionary attacks” from a practical standpoint. Simply put, this is where an attacker typically captures the token and enough other information (perhaps by eavesdropping a transaction) to go back to her own computer and quickly search through all possible PIN numbers until she finds the unique PIN consistent with the captured information. To this end we must assume that an attacker has access to some cipher text encrypted with the finally agreed key, which, when decrypted with the correct key, results in something instantly recognizable. In other words, an attacker will know when they have hit on the right key. M-Pin negates this attack because it leaks no information about the token in a way that could be used to reverse engineer the pin.

The M-Pin Server itself also employs a number of counter measures, such as a strict “three strikes” rule, whereby the user is only allowed three chances to authenticate to the service before their account is de-activated. A number of other fraud detection and real-time analysis techniques are also implemented, including geo-location awareness.

Another top security consideration is whether M-Pin can withstand man-in-the-middle (MITM) or man-in-the-browser (MITB) attacks. In the scenario where an attacker is intercepting traffic between the authentication service and the client (a man-in-the-middle or MITM), M-Pin employs HTTPS to encrypt the traffic. Further, the M-Pin pin pad reveals no information about the token or the user’s 4-digit pin, which is never sent over the wire.

In the scenario where an attacker has malware installed on a user’s machine to perform a MITB attack, the malware and level of compromise would have to be severe and directly targeted; the malware would have to compromise the browser’s integrity, removing and exporting the user’s token out of the browser’s storage, in effect, re-writing the code of the HTML5 browser to enable some kind of token export (without the user knowing). Of course, that’s only one part of the equation. In order to get the user’s 4-digit PIN, the malware would also have to screen capture or screen record the user’s computer. Note that traditional key logging will not capture a 4-digit PIN as M-Pin pin pad rejects any input not directly from the mouse pad or touch input device. Finally, the elliptic curve cryptographic code would need to be run independently from the pin pad, in effect, performing the functions of the M-Pin pin pad exactly; this is not a trivial undertaking in and of itself. Finally, the attacker would need to circumvent the other counter measures employed within the M-Pin Server to detect such attacks.

Code

The cryptography described herein is powered by MIRACL, an open-source cryptographic library available for download at www.certivox.com. If you require a commercial license outside of the scope of the AGPL license, please contact sales@certivox.com.

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635

Patents

M-Pin utilizes a number of patent-pending and patented technologies of which CertiVox is the exclusive licensee; EP Patent No. 1 730 88 (EP Application No. 05718824.5) granted by the European Patent Office on 13th October 2010 for “Verification of Identity Based Signatories” and US Patent No. 7,860,247 granted on December 28th 2010 for “Identity Based Encryption”.

T: +44 (0)20 3191 8294 | E: info@certivox.com | www.certivox.com | 81 Rivington Street, London, UK, EC2A 3AY. Registered in England & Wales 7017635