iDKI

ADVANCED AUTHENTICATION, SIMPLIFIED

# DATASHEET: iDKI

# (Identity Key)

**DOCUMENT CONTROL**

Concept Document: **2016 / 05 10**

Version Number: **01**

Issue Date: 2016 / 05 16

Presented by: Stefan van Wyk

**CONFIDENTIALITY**

**STATUS: CONFIDENTIAL**

# OVERVIEW

Pramosa's iDKI (Identity Key) addresses the most fundamental part of security in the simplest of fashions, namely that of advanced user authentication through the power of universal 2nd factor (U2F) elliptic curve encryption.

The Authentication Server, a *free* server software component, is deployed to serve as authentication proxy close to the Active Directory, with simple Group Policy distribution of the iDKI Client Package. The entire solution can be deployed for Workgroups as well if there is no Active Directory deployed.

Organizations can easily distribute U2F keys to users in a fishbowl distribution method where keys are only associated with a specific user upon registration – a simple 2 minute procedure for a user to enrol and bind a key to his user profile.

# BENEFITS

Benefits of deploying iDKI as a U2F advanced authentication method includes:

- Ease of deployment: software and tokens are rolled out to users with no interference to normal business operations.
- Efficient management: Users self-enrol on the system, relieving administrative overhead for deployment and continued operation.
- Reduce IT costs: No additional staff (administrative or helpdesk) is needed. In fact, users can assist themselves with password management by resetting their domain login passwords directly from their Windows login screen without the assistance of a call centre or helpdesk operator.
- Protection from phishing. U2F, unlike nearly all other multifactor authentication systems, such as mobile device applications making use of PINs or passwords, are not open to phishing methods!
- U2F keys can be purchased anywhere in the world as well as online, so availability and shipping globally enables ease of deployment for clients with a global footprint.
- Ease of compliance with audit requirements, as each login is unique, relieving the stress from users on overbearing password complexities
- Scalability. iDKI efficiently caters for very small deployments of 10 users to large enterprise with large AD domain structures, as well as multiple domain deployments.

# WHY U2F?

Complexity and password volume results in a password complexity paradox, where security starts to decrease due to users finding alternative ways of remembering passwords (notes, spreadsheets etc.). The familiar problems with passwords are that they are reused across multiple sites and applications, both internally as well as externally, they are phished easily, are prone to Man in The Middle attacks and can easily be key logged.

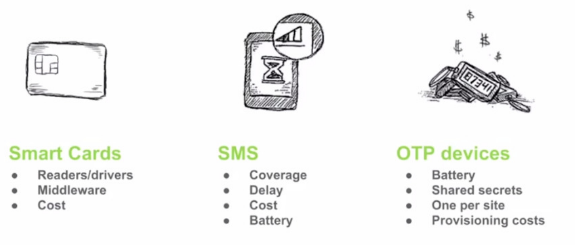
Reused

Phished and MitM

Keylogged

One might ask if we have not solved this already with smartcards, mobile applications, OTPs etc. Some problems with these are:

Smartcards – must have separate readers, drivers, middleware, expensive for all users. Each 'application' of the concept needs a separate smartcard.
SMS – suffers from coverage, delay, cost, and is impacted by battery uptime.
OTP devices and Mobile applications: Battery uptime, shared secrets, one per site, and high provisioning costs. In addition, many users do not want corporate applications on their personal smart phones without being subsidised on phone and data costs.



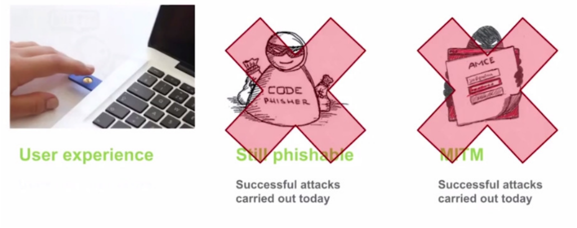
BUT most importantly:
The above methods typically result in bad user experience's and causes friction. These methods to authenticate are also still phishable (all except smartcards) and MiTM attacks are still used against them.

875???
User experience
Users find it hard to use
CODE PHISHER
Still phishable
Successful attacks carried out today
ACME
MITM
Successful attacks carried out today

Over 90% of all hacking attacks begins with phishing! There is always someone in your organisation that is phishable, if not most of them.

Universal 2$^{nd}$ Factor (U2F) solves all these problems:

- Great user experience
- Is Not phishable
- Has built-in MiTM protection

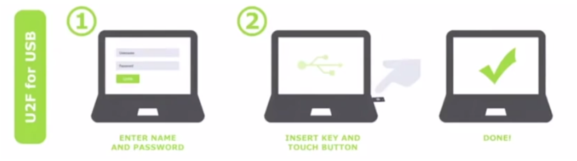

User experience
CODE PHISHER
Still phishable
Successful attacks carried out today
ACME
MITM
Successful attacks carried out today

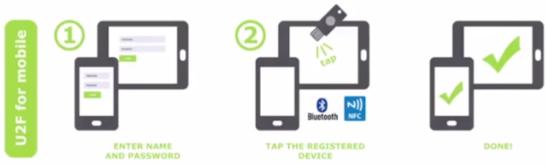
ALSO – no batteries and no drivers needs to be installed.

One device securely works with to multiple sites/applications with site-specific keys.

U2F is an Open standard by the FIDO Alliance.

U2F ensures that both the user as well as the server has to authenticate themselves during the communication process, with unique private and public key pairs created for each application by the key, ensuring complete security between a specific user and an application, with no risk of cross-pollination of security information between applications. With each authentication being asymmetric, unique and both user and server/application having to authenticate, phishing and MiTM is effectively neutralised.





The top user globally at the moment is Google themselves. Google started converting to U2F since 2014, and now has most if its internal applications converted to U2F. Google have moved away from using its own smart phone authenticator to making use of U2F keys and the U2F standard as method of choice to all its internal applications.

Below are some statistics from Google on its success:

- Support incidents have decreased by 70%
- Average login times are 53% faster moving from OTP via mobile application to U2F tokens
- Security incidents had a "dramatic decrease"

# FEATURES

## ACTIVE DIRECTORY INTEGRATION

The Authentication Server is deployed autonomously from the Active Directory Server – therefore no AD changes are needed. Up to five AD servers can be defined to support the hierarchical structure of AD servers deployed in multiple locations.

The system caters for single domains, multi domains as well as Workgroups.

## CENTRALIZED U2F AUTHENTICATION

iDKI has been developed explicitly around the emerging gold standard of authentication, namely Universal 2nd Factor. User authentication can hereby be developed into a federated system where all user access (physical and logical, as well as on premise and cloud) can be controlled from a single point, using the strongest method of advanced authentication currently available.

U2F, by standards definition, creates separate private and public key pairs for each application, including web applications and even websites. Keys cannot be copied or moved from either the source (user) or the destination (server). Each key pair, making use of elliptic curve cryptography, is therefore unique and cannot be used anywhere else. The U2F keys therefore becomes a key holder that creates virtual keys for each application. Upon authentication, the server or application first has to prove its own origin before the U2F enabled key will allow signing to authenticate, which is then accepted by the server or application. Unique to the U2F standard is therefore the requirement to authenticate both ends of the transaction, the user as well as the server or application before the connection is established to grant a user access to the systems.

The most important benefit of this mechanism is that it protects the U2F solution from all phishing attacks, which is how 90% of all network attacks is started – as phishing attacks on unsuspecting users.

## OPEN STANDARDS BY THE FIDO ALLIANCE

Universal 2$^{nd}$ Factor (U2F) is an open standard developed and hosted by the FIDO Alliance, a global alliance set up to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. The Board level members of the FIDO Alliance includes, inter alia, Microsoft, Google, MasterCard, VISA, PayPal, Bank of America and Yubico.
In 2 years FIDO Alliance membership has grown from just 13 to over 200 global companies.

## USER SELF-SERVICED PASSWORD MANAGEMENT

Users can manage their own AD passwords directly from their Windows Login screen without the need for additional portals or mobile applications. A single user friendly interface is thereby used for login via U2F, resetting of AD passwords as well as requesting of fall back OTP in case their Yubikey's are not available.

This relieves the additional overhead for IT support that often goes hand-in-hand with Active Directory deployments to administrate user passwords.

## OTP FALLBACK BASED ON THE U2F SPECIFICATIONS

Making use of fall back to one-time-pins (OTP) is enhanced by having developed OTP based around the U2F standard. An OTP can only be used on the specific registered device (Windows workstation or laptop). Phishing the OTP is devoid of value, as it can only be used from the user's device, and from nowhere else.

## INTEGRATED REPORTING

The Authentication server provides a predefined set of customizable reports that allow you quickly view summary information, such as identifying users making use of OTP instead of their tokens on a regular basis or reviewing authentications by users.

## CENTRALIZED MANAGEMENT

Users can be blocked or required to re-enrol directly from the Authentication Server instantly.

Re-enrolment effectively and efficiently 'deletes' the previously registered key and replaces it with the new one.

## BUILT IN ADMINISTRATIVE USERS AND ONLINE HELP

Upon deployment, specific keys are set as administrative keys that are held in custody by the IT department. Without the need for registration on all devices, these administrative keys can access all machines that are registered on the system to ensure operational support access for the IT administrative support team.

A full online help is available via the web administrative portal to ensure that administrators have all the help documentation at their fingertips.

## ACTIVE-SYNC SOLUTION

In addition to resolving authentication and password management, iDKI also offers the ability to avoid account lockouts when users use multiple devices, such as mobile, to access their email. Account lockout occurs when a user changes their passwords on AD via their laptops or workstations, only to have themselves being locked out when they start up their mobile devices to check email, as these have the old passwords that results in too many login attempts to the mail server – resulting in the user account being locked on the Active Directory.

IDKi-Sync, deployed as an extension to IDKi, avoids this automatically across common mobile platforms (Windows, IOS and Android) by ensuring that all the devices are updated with the correct login password credentials.

### AUTOMATED SYSTEM UPDATES

Updates to the user credential provider is distributed quietly in the background to all users upon login. The next time they log in, the new credential provider will automatically replace the older version.

This minimizes administrative overhead to manage the system and ensures that all users are always on the latest version of software.

### GLOBAL SETTINGS AS WELL AS GROUP OR INDIVIDUAL OVERRIDES

Deployment settings are done on a global scale, for example, enable or disable OTP or email as fall back, or set the validity time of OTPs to 5 minutes.

All the settings can be customized globally or made applicable to specific AD groups based on OID, or even to specific users individually. Enterprise deployments can therefore be managed globally or individually based on AD credentials and groups, making the iDKI solution a perfect fit for any organization.

## YUBIKEY OPTIONS

The following Yubikeys are fully supported by iDKI, that is all U2F capable Yubikeys:

FIDO U2F Security Key

Yubikey 4

Yubikey Neo

Any of the nano versions (small nano form factor) can also be used.
Also note that the same key used to authenticate corporate logins can be used for personal accounts, such as gmail, Dropbox and Github. By extending their advanced authentication footprint into their personal domains, users extends their

privacy by defending against phishing and other poorer authentication schemas.

# FEITIAN OPTIONS

Feitian U2F NFC keys that are supported are the K9 keys. They work natively with the iDKI solution and is very cost-efficient for larger deployments as well as where NFC is required for mobile devices.

# CLOSING

Unlike other authentication methodologies that has a one-to-one relationship between method and application, U2F keys have one-to-many relationships, where the same key can be used to secure a multitude of applications and websites.

With the authentication server being *free*, deployment costs are limited to the user seats and a minimal annual license, making it a very cost efficient solution with rapid-time-to-deploy capability so that the organisation can experience real benefits almost immediately.