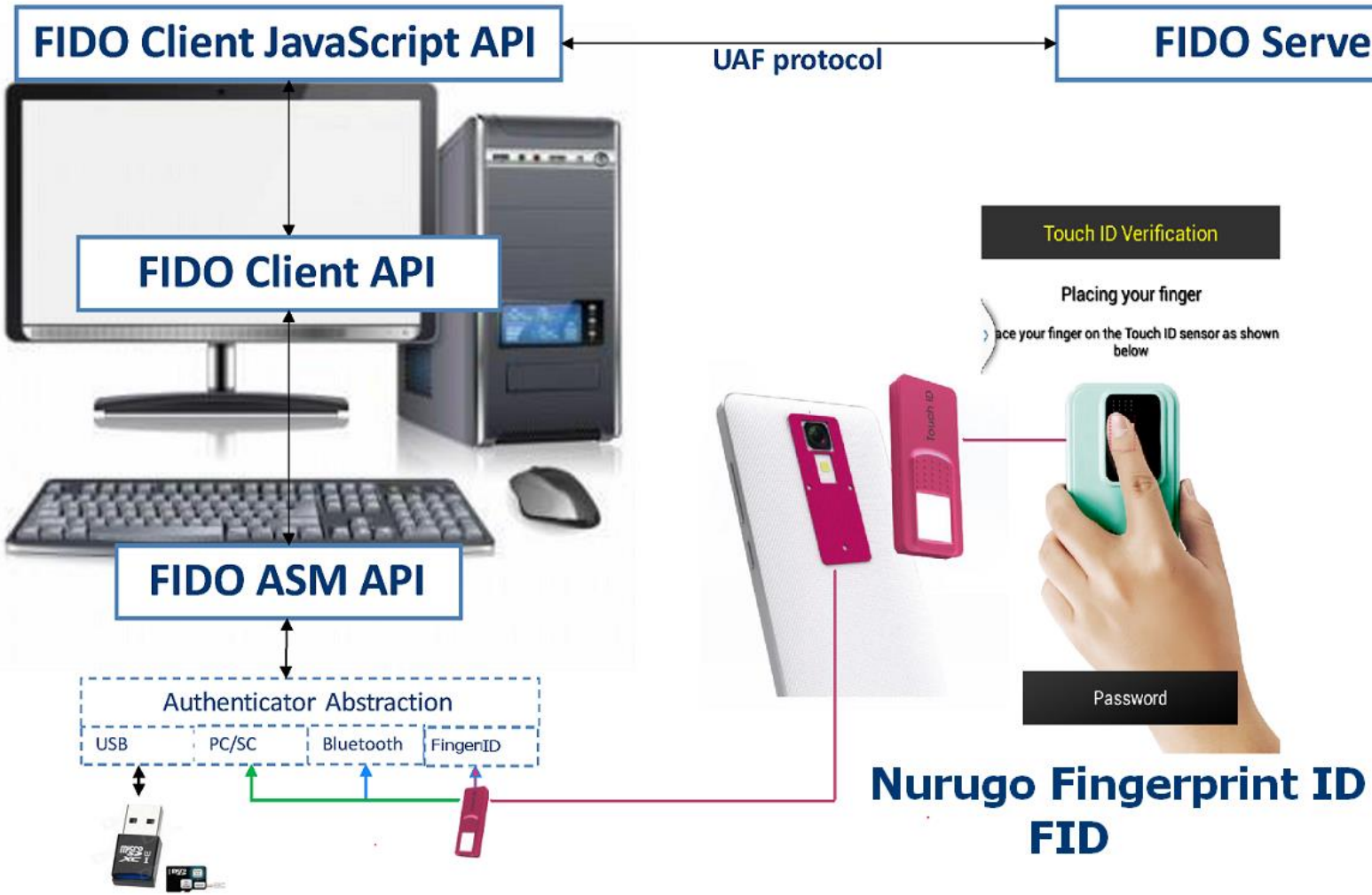
Creating PKI with patented Nurugo© - FidoScrypt© Biometrics Technology

U2F - using Nurugo Biometric as second factor authentication token

Passwordless Authentication with patented Nurugo FID

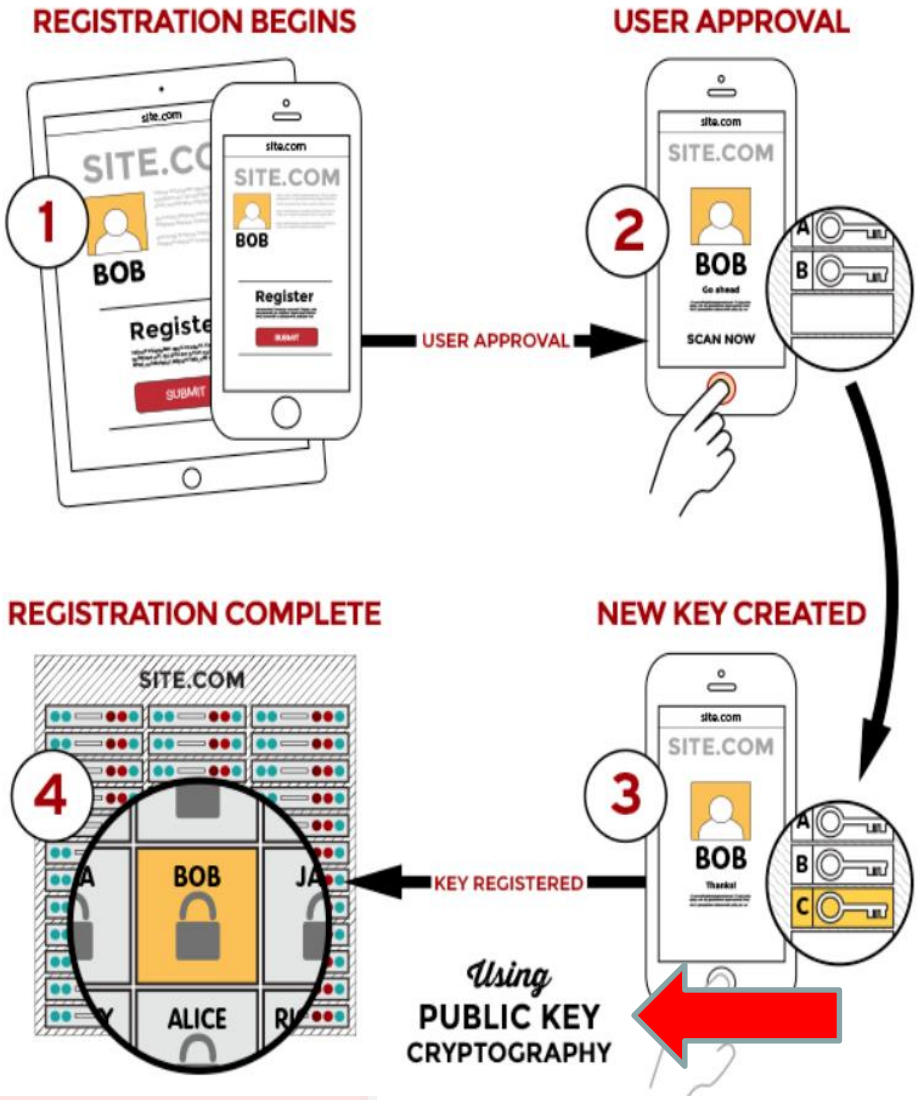


What is the difference and advantage of using FidoScrypt

- **The FidoScrypt based U2F uses standard public key techniques to provide unbreakable identification – authentication.**
- **During registration with an online service the user CLIENT device creates locally (not on cloud servers)a new key. It retains the private key and registers the public key with the online service's Fido component.**
- **The new and patented part is, that the private key is generated by the users Fingerprint, using the Nurugo Biometrics technology, identifying the USER unmistakably.**
- **Only then Authentication is done by the client device proving possession of the private key to the service by signing a challenge.**
- **The challenge again is done by Fingerprint ID, but … remember to protect the identity and verify the authentication of the user, another local created PKI is used instead of a Fingerprint file that could be tempered with.**
- **Nurugo uses the Fingerprint scanned by a high resolution camera of the device and saves it as an encrypted image, which cannot be copied or tempered with.**

Principles of creating secured access YES and NO's

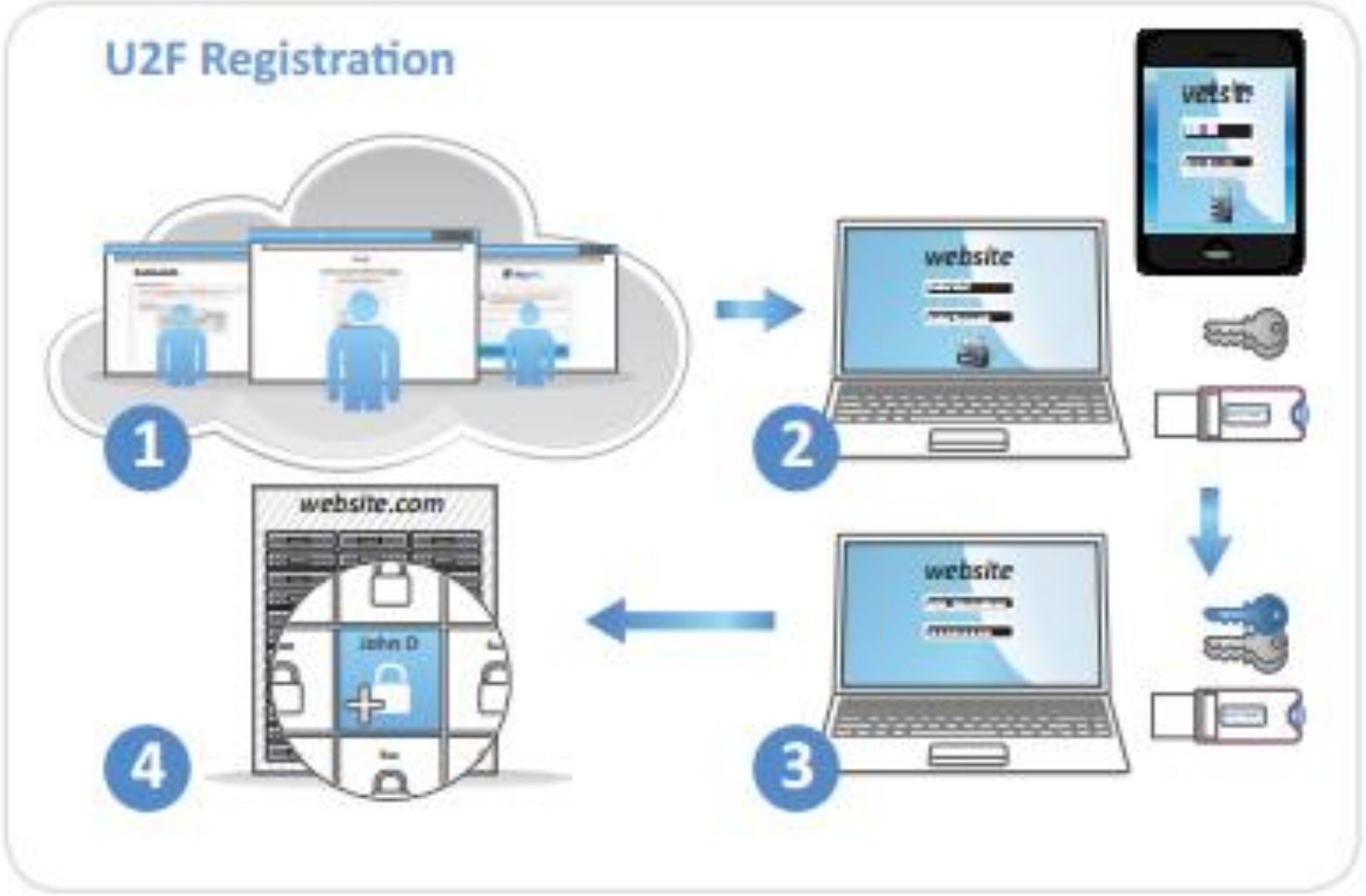
- **Apple Iphone uses a sensor approach of Fingerprint ID, with a sensor area much to small to comply with International regulations. It also stores the FID file locally and on the insecure Apple Cloud, making this method totally open to copies and hacking.**
- **Other devices uses the touch screen scanning method, even worse, the fingerprint is available as residue on the screen and in clear data stored in the device, open for easy copy and hacking.**
- **The FidoScrypt Nurugo technology uses the actual Fingeprint Image, in a patented way optical scanned by the Camera of the device, and stores the Data locally encrypted as PKI, making it absolutely impossible to break!**



- The clients private keys can be used ONLY after they locally identified the correct user (Person) and then unlocked the device and transaction.
- The local unlock is accomplished by the user friendly and highly secured, patented Nurugo process as second factor authentication. So FidoScrypt works with double security, first as Person Identifier, then as second factor authentication.
- The copyrighted FidoScrypt protocols are designed from the ground to and identify the User, protect and identify the correct device, making Passwords redundant. No New Servers systems are required , Fidoscrypt ads a software component to the existing server user base. Since PKI is used existing user names can be changed by the user frequently, passwords are not required anymore.
- This way the authentication, transaction approvals, identification etc. becomes 100% secured, cannot be hacked (as no Files or Data are hosted anywhere) all process is done locally in the device and at the end of each process all traces are deleted.
- SSCSIM (Encryption embedded into the SIM card) adds a new until now unknown grade of Security to the process.
- The FidoScrypt Nurugo technology uses the actual Fingeprint Image, in a patented way optical scanned by the Camera of the device, and stores the Data locally encrypted as PKI, making it absolutely impossible to break!
- These protocols do not provide any information that can be used by a different user, service or hacker, cannot track a user across the service

U2F Registration process flow

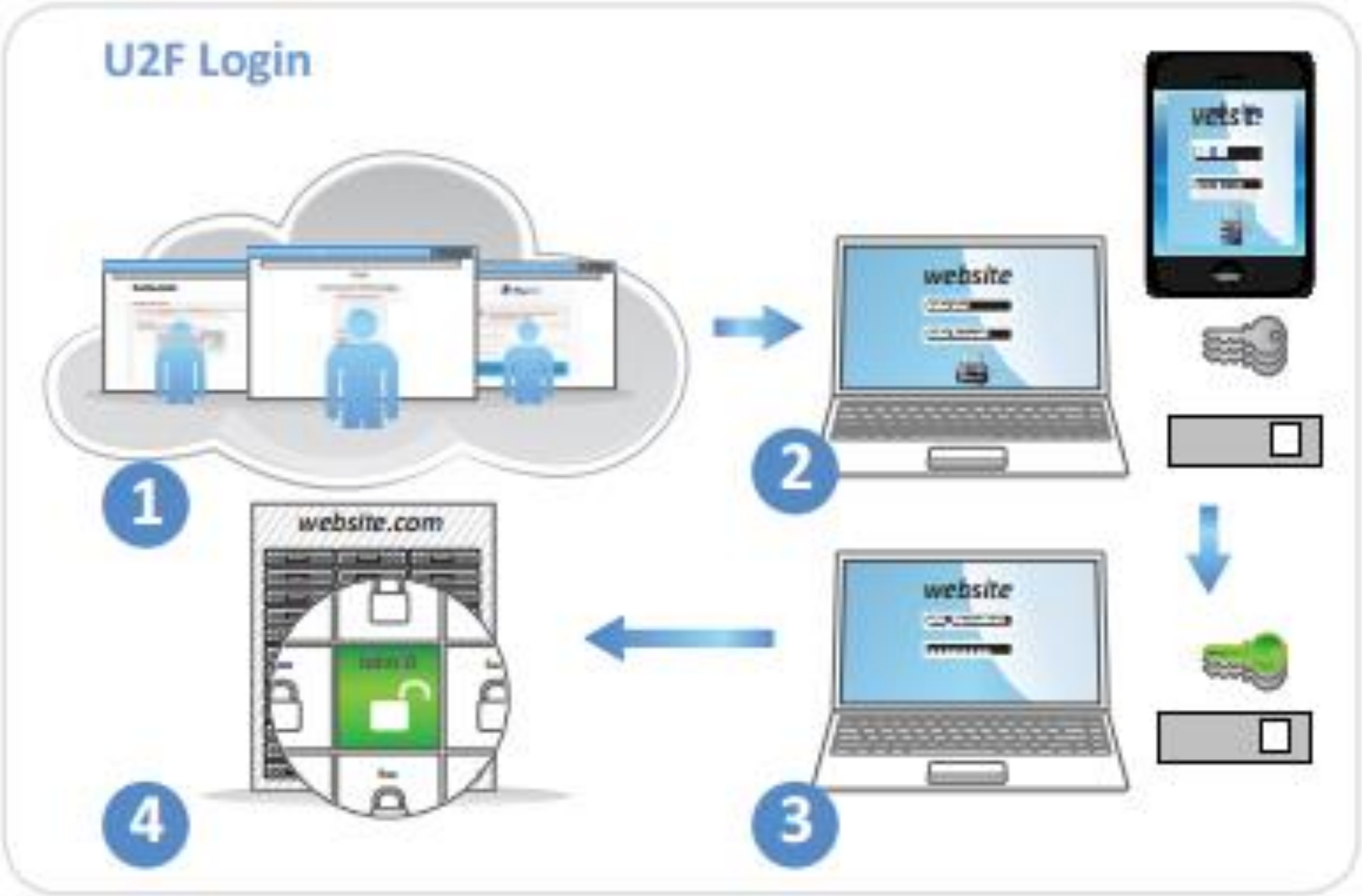
- User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
- User unlocks the FIDO authenticator using a fingerprint reader, a button on a second–factor device, securely–entered PIN or other method.
- User's device creates a new public/private key pair unique for the local device, online service and user's account.
- Public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

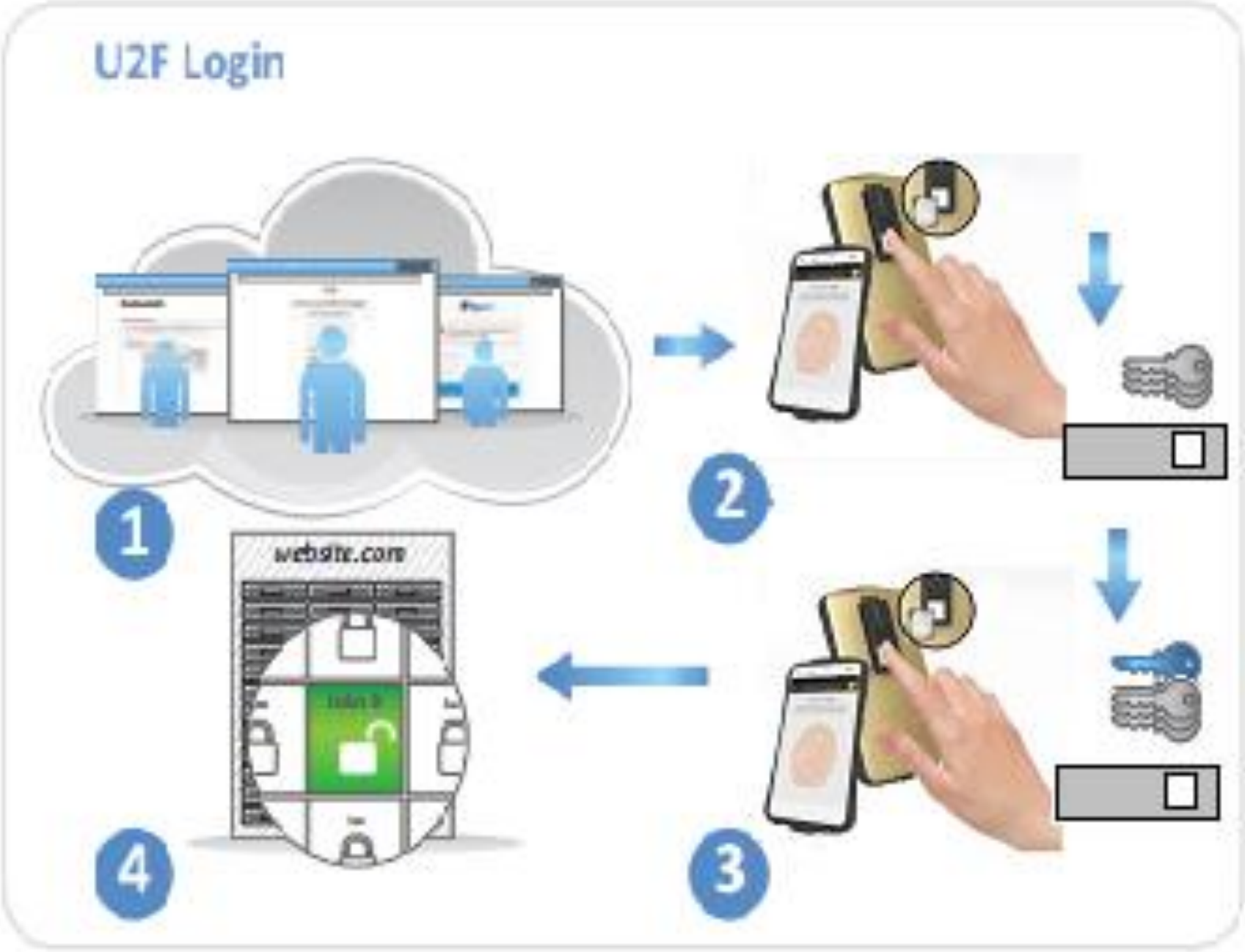

U2F Registration
website
website
website.com
john D
1
2
3
4

U2F Registration

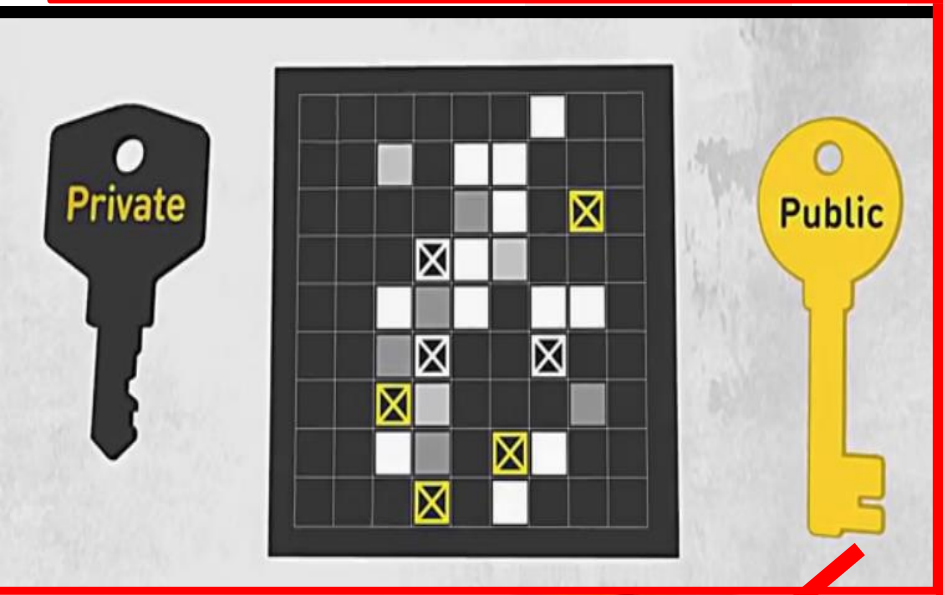
U2F LOGIN process flow

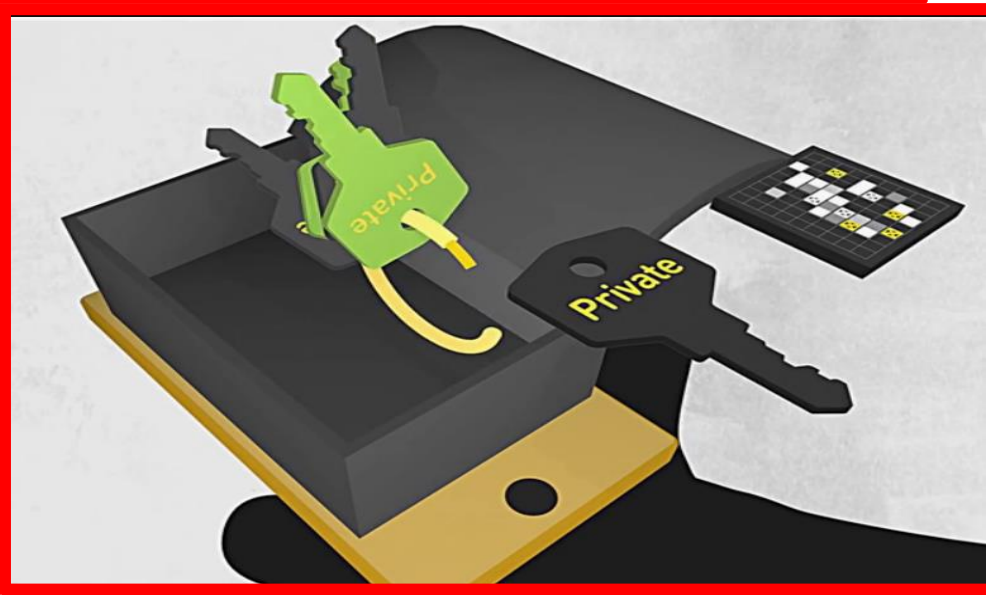
- Online service challenges the user to login with a previously registered device that matches the service's acceptance policy.
- User unlocks the FIDO authenticator using the same method as at Registration time.
- Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge.
- Client device sends the signed challenge back to the service, which verifies it with the stored public key and logs in the user.


U2F Login
website
website
website.com
1
2
3
4


U2F Login
website.com
1
2
3
4

Bio Sensor + PKI = Nurugo (FIDO)





Authentication Server

Tokenization with Dynamic code(OTP) =

"B9E2995B2B7602AE825CE7DE819F10
F088419E595A9AAE81919EF58"

APPLE Fingerprint ID with NURUGO

Store Mac iPhone Watch iPad iPod iTunes Support

Apple PKI

Apple established the Apple PKI in support of the generation, issuance, distribution, revocation, administration, and management of public/private cryptographic keys that are contained in CA-signed X.509 Certificates.

Apple Root Certificates

- Apple Inc. Root Certificate
- Apple Computer, Inc. Root Certificate
- Apple Root CA – G2 Root Certificate
- Apple Root CA – G3 Root Certificate

Apple Intermediate Certificates

- Apple IST CA 2 – G1 Certficate
- Apple IST CA 4 – G1 Certficate
- Apple IST CA 5 – G1 Certficate
- Application Integration Certificate
- Application Integration 2 Certificate
- Application Integration – G3 Certificate
- Developer Authentication Certificate
- Developer ID Certificate
- Software Update Certificate
- Timestamp Certificate
- Worldwide Developer Relations Certificate
- Worldwide Developer Relations – G2 Certificate

PKI (ITU X.509) Structure using Fidoscrypt

< Before user registration >

Public Key Certificate

Version / Serial Number / Signature algorithm / Hash algorithm / Issuer Name / Validity Period / Public Key

Subject Distinguished Name / Subject Public Key Information / Issuer's Signature

Extended Validation

(Empty)

< After user registration >

Public Key Certificate

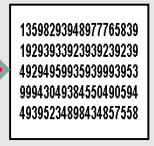
Version / Serial Number / Signature algorithm / Hash algorithm / Issuer Name / Validity Period / Public Key

Subject Distinguished Name / Subject Public Key Information / Issuer's Signature

Extended Validation

- **Biometric Code + at least one of Additional Code**

"B9E2995B2B7602
AE825CE7DE819F
10F088419E595A9
AAE81919EF58



Bar Code/ QR / UPC / RFID / URL /CRL / PUF/ GS1/ GSIN / IPv6 / MAC / MAC/ Cryptographic hash functions address/ unique identification information etc.

Muiti Application on e-ID (Examples)

Multi App

1 App	3 App´s	5 App´s	10 App´s
eService	eService eHealth eTicketing	eService eDL eGate eBanking eLibrary	eID eService eHealth eTicketing ATM eDL ePurse eGates Travel document
Example	Finland FINID	Italy CNS	Hong Kong HKSAR	Malaysia MyKad

NuRugo Biometrics (Example)

UBIQUITOUS AUTHENTICATION MANAGEMENT

National ID	Government Intelligent Services	Medical	e-Voting	Pension	Passport ICAO	Bank	Physical Access /Smart Car	PC/ Cloud Logon	Smart Phone / Smart Home
PKI + Data	PKI + Data	PKI + Data	PKI + Data	PKI + Data	PKI + Data	PKI + Data	PKI	PKI	PKI

Physical unclonable functions

Network Authentication .....

Multi Bio Combination Nurugo-Fido

Diverse combinations of Biometrics

Combination 2 more finger	Combination 1 finger + IRIS	Combination Iris + Vein	Combination Iris + Facial	Combination Finger+ Sign	Combination Voice+ Facial	Combination with each Palm/ Blood / Voice / DNA / Keystroke etc.

Allocated purpose of use

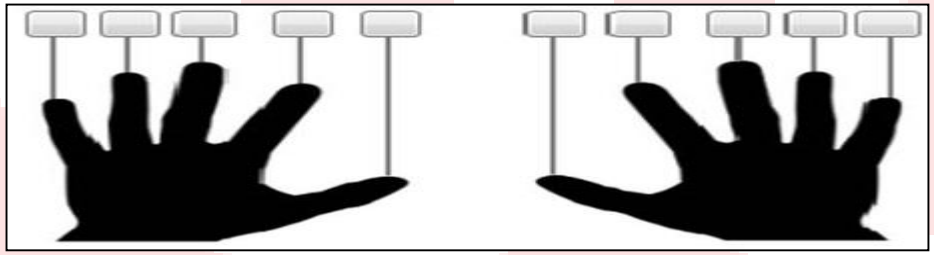
Application Services

Bank/ Credit Card ↔ Payment ↔ Government ↔ Internet ↔ Cloud ↔ Car ↔ IoT ↔ 911 ↔ Emergency

Allocated purpose of use

Government ID

Device / User Security

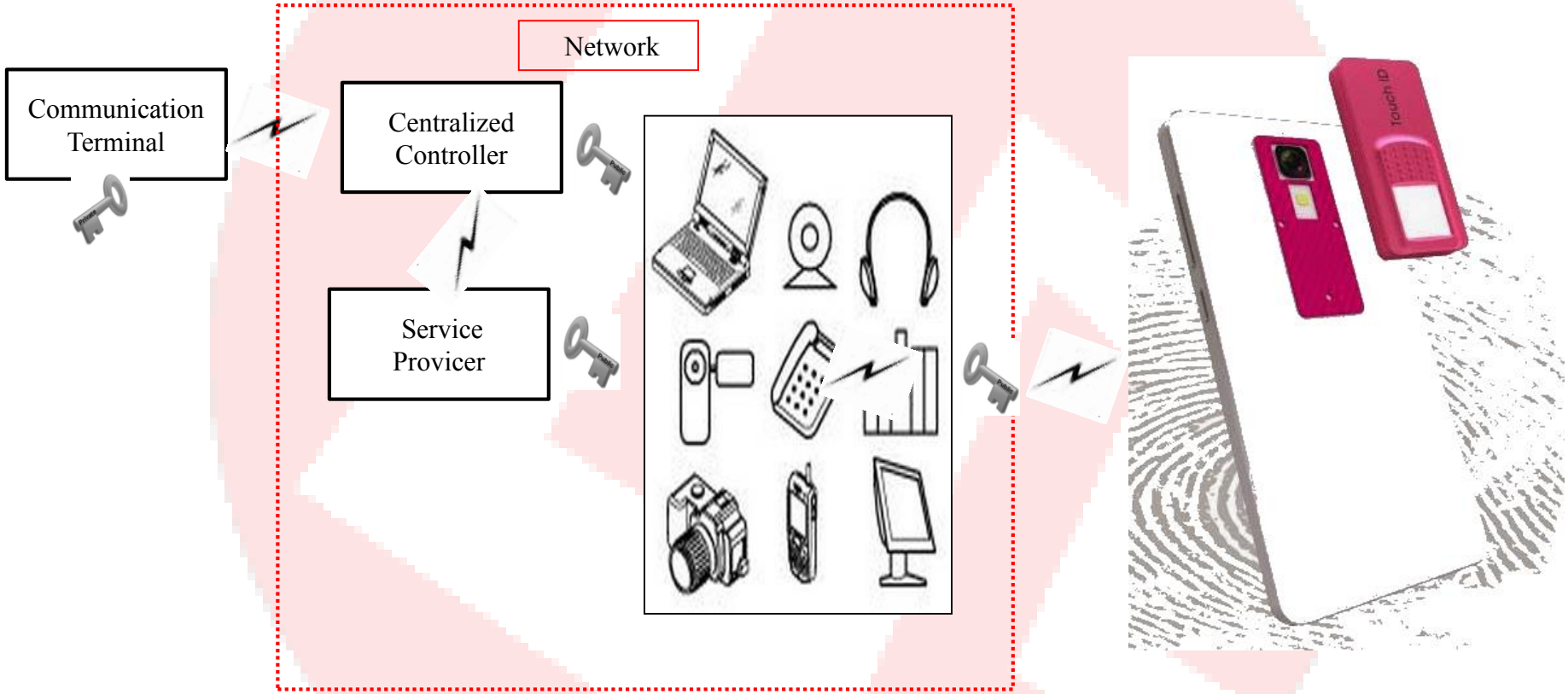


Payments

Internet - Banking

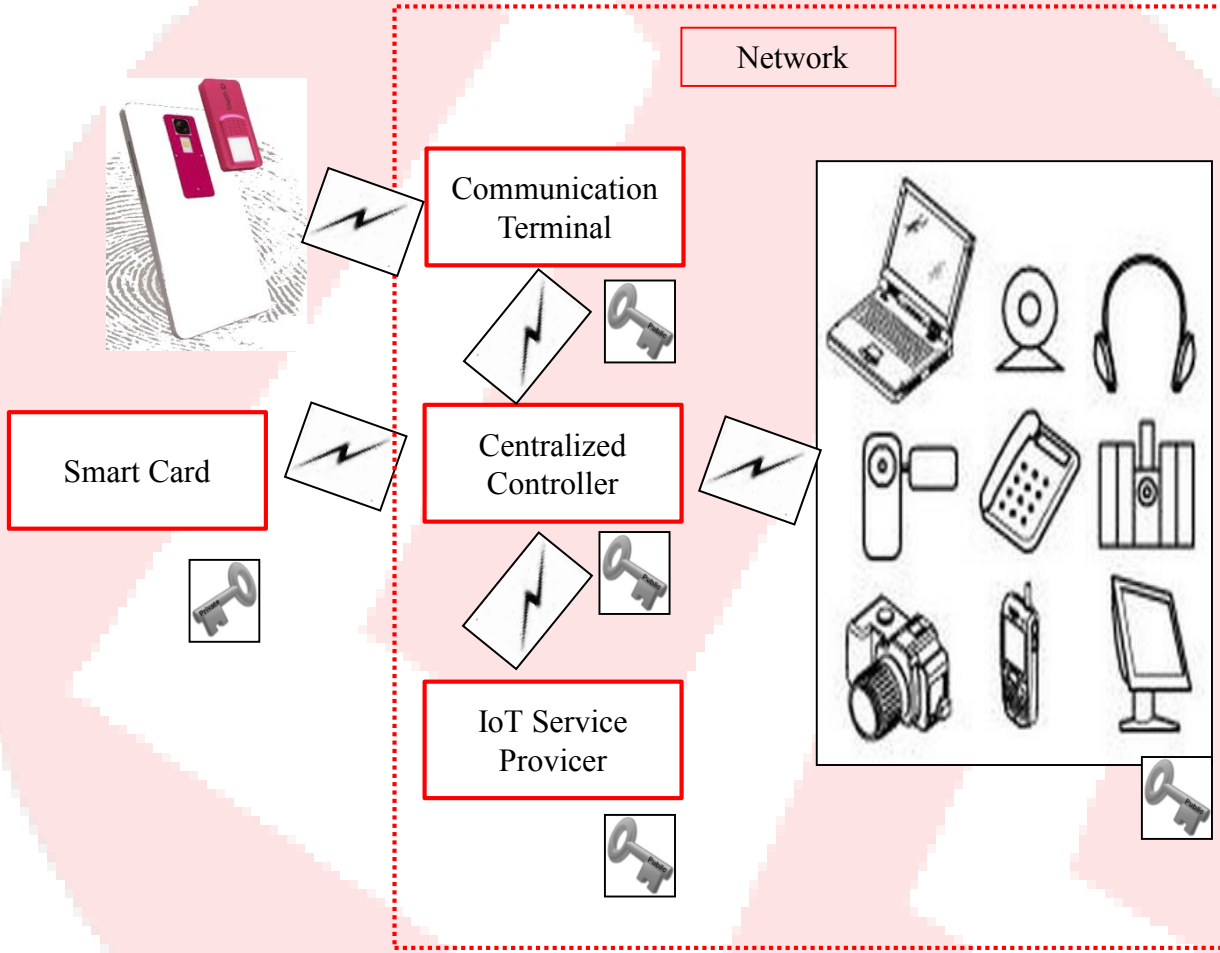
NURUGO patented Multi Finger Authentication

Authentication Key created with Nurugo Fidoscrypt in Smart Phone



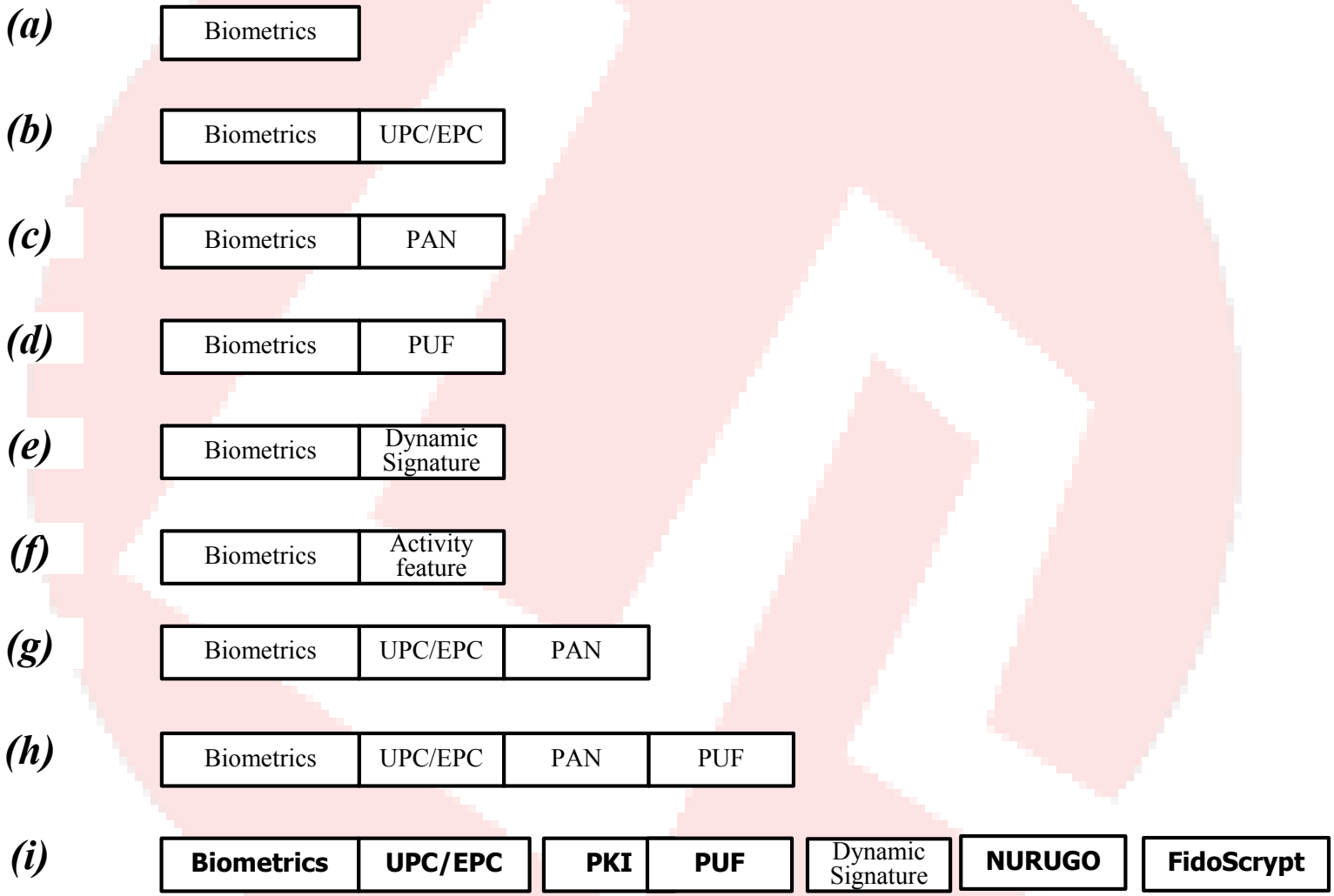
Personal | **Company** | **Government** | **Bank**

Authentication Key for National ID

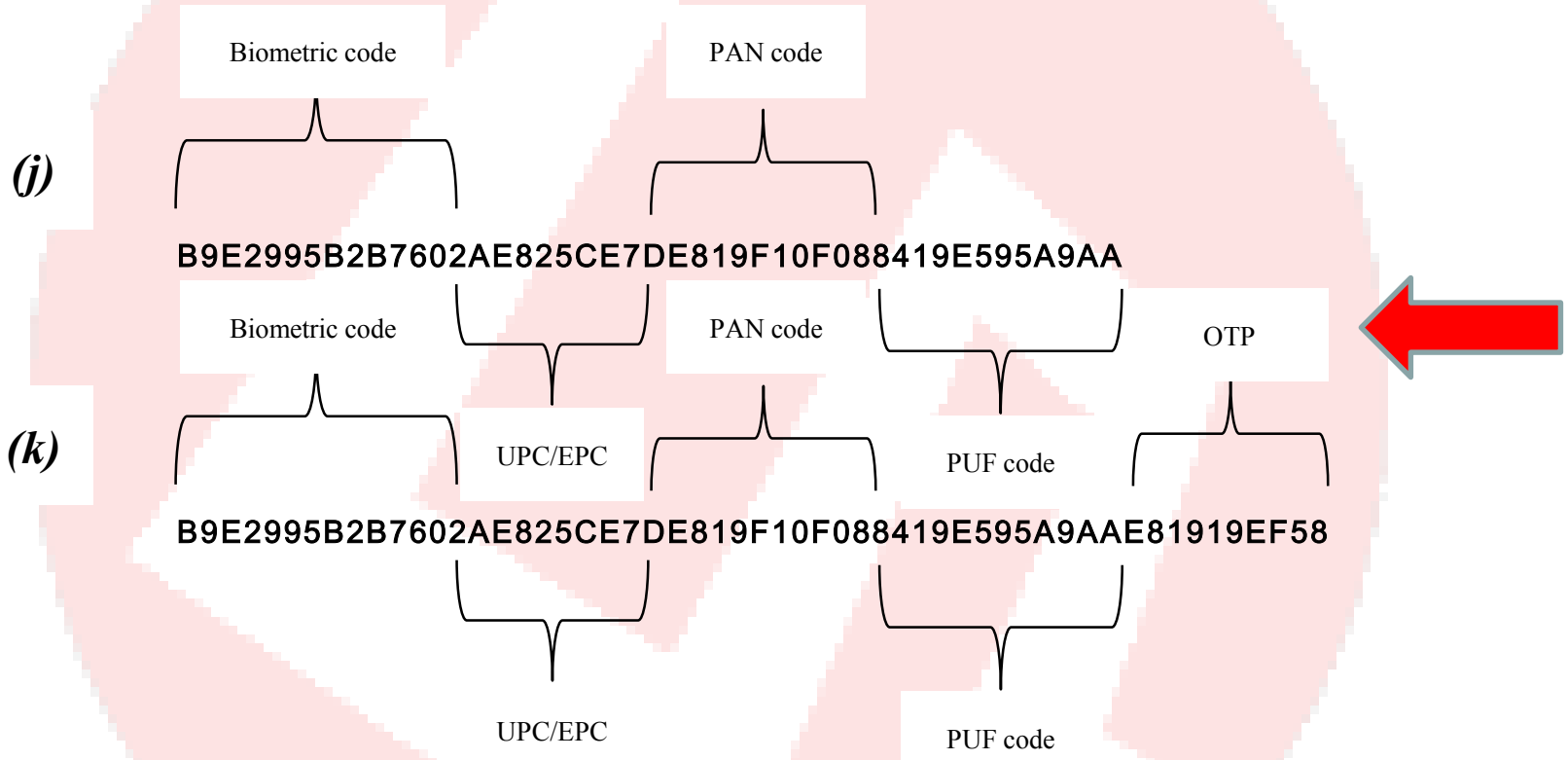


SingPass | **Password less** | **Smart Device** | **authenticate**

Why has Nurugo the highest Security

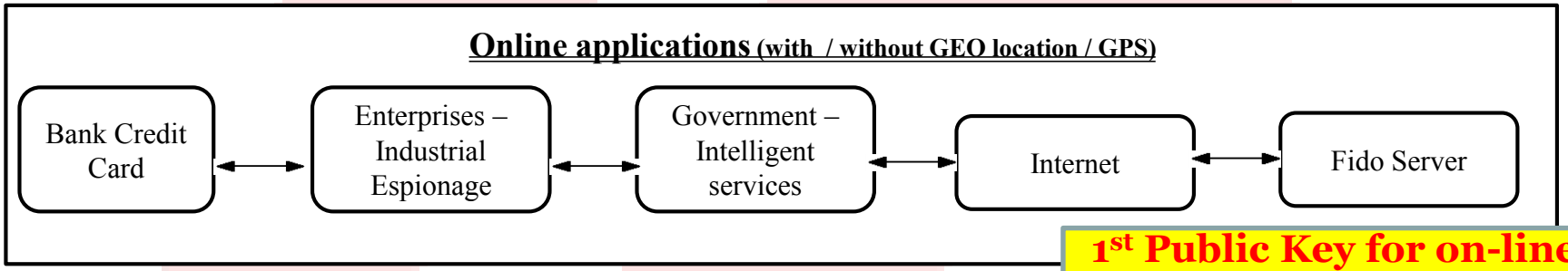


FidoScrypt Authentication Code Format



NURUGO +	FidoScrypt =	PKI	authorize

On-line & Off-line Authentication



1st Public Key for on-line at Fido Authentication Server

Off-line application support for each service etc. by Government & Financial Authority

Bio Sensor on ATM for cash withdrawal etc.	**Bio Sensor on POS** for buy food etc.	**Bio Sensor on Centralized Controller** for control IoT Devices etc.	**Bio Sensor on Smart Card/Phone** for Identification and Authentication of Encryption processes for all levels of Security.

2nd Public Key for off-line for ATM, POS, Centralized Controller, Phone/Card

Store with Private Key at Mobile Device locally – use online P2P

Key Distribution Example

PKI generated with Nurugo

Public Key

Private Key

FIDO Server

"B9E2995B2B7602AE825CE7DE819F10F

Government Public Key α

shopping Public Key α

Bank Public Key α

Access ID Public Key α

"B9E2995B2B7602AESHE653HD83MK82S

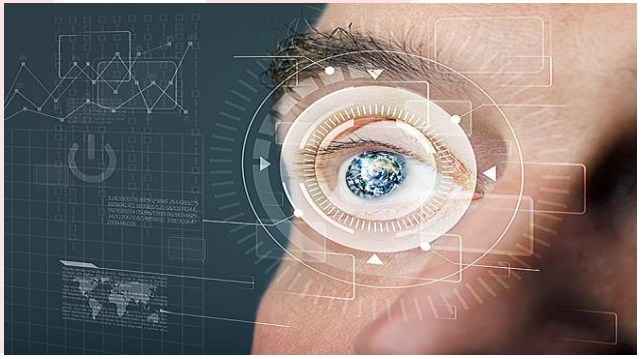
Public Key β

Stored in Smart Device / Phone

Private Key β

FidoScrypt Solution TRIPPLE Security

- Biometrics data acquisition module
- Biometrics data management module
- Key management module
- Biometric authentication module
- VPN management module
- Authentication execution module
- OTP generation module
- Device data acquisition module



Why is FidoScrypt with Nurugo the most secure Access authentication and Identification ?

- Nurugo's patented Smart Device FID
- Nurugo's patented "ANTI WET" Finger ID
- 100% Secure against copy and hacking
- No cloud storage of any Keys or information
- PKI will only be used once on each Transaction
- FidoScrypt uses SecureScrypt encryption AES 256
- No records or logs means no copies or hacking
- all transactions done P2P
- Copyrighted Tripple authentication
- Optional embedded structure in SIM card for Device Security
- Easy implementation into existing authentication systems, no new hardware required.