IAP800

IAP800®
Piattaforma Innovativa per l'Autenticazione Forte
e l'Antifrode

Ireth

AUTENTICAZIONE FORTE & ANTIFRODE

La Piattaforma IAP800®

Autenticazione Forte & Antifrode

IAP800

IAP800® è una piattaforma di Autenticazione Forte utilizzata ormai da milioni di utenti.

IAP800® è ideale non solo per l'autenticazione forte ai servizi *"mission critical"* quali, ad esempio, l'*home banking* secondo gli standard SCA PSD2, ma anche per la strong customer authentication di servizi *"aziendali",* garantendo accessi remoti sicuri alle risorse aziendali per dipendenti e collaboratori, necessità sempre più diffusa, considerata la crescita esponenziale dello smart working.
IAP800®, oltre ad essere robusta e affidabile, è una piattaforma completa, sia lato server, grazie a solide componenti infrastrutturali, che lato utente, grazie ad una varietà di dispositivi di autenticazione software e hardware.

La soluzione IAP800® è conforme agli standard di autenticazione forte OATH (Open Authentication) e FIDO (Fast Identity Online), gestendo dunque sia autenticazioni *one time password* che *passwordless,* attraverso il riconoscimento biometrico automatico vocale, facciale o fingerprint dell'utente.

Il Server IAP800® è sviluppato su appliance dedicate, ottimizzate per le attività di autenticazione massiva e profilazione degli accessi degli utenti.

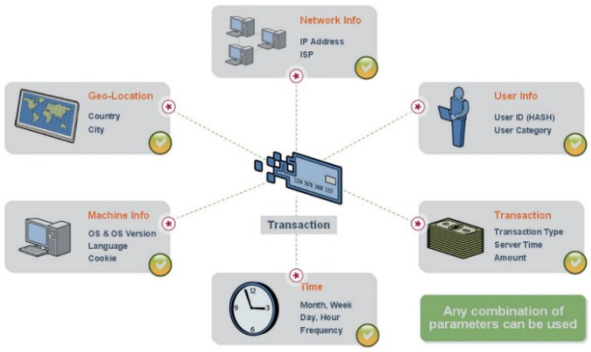
Può facilmente scalare in strutture cluster con più appliance multi-active, per garantire sempre ed in ogni circostanza la *massima disponibilità del servizio.*

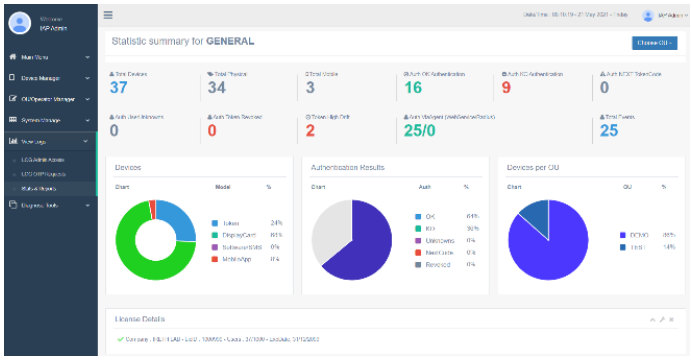
Oltre alla gestione della Strong Authentication, il server IAP800® è dotato di una *potente funzionalità antifrode*, in grado di garantire il più alto livello di efficacia oggi raggiungibile da qualsiasi altra soluzione.
IAP800® riesce infatti a contrastare perentoriamente qualsiasi malware tramite una disintermediazione tra il canale di autenticazione e il canale autorizzativo della transazione.

Questo grazie alle AFC800™, innovative carte NFC con software antifrode prodotte e brevettate da IRETH, carte che, una volta poste in prossimità del mobile/pc, instaurano un canale assolutamente inattaccabile tra server e client, legittimando la firma della transazione e garantendo l'inviolabilità della transazione.

IAP800®, come ulteriori strumenti di supporto per il contrasto delle frodi online, include il modulo Sys Log di Auditing delle autenticazioni effettuate, e, opzionalmente, il modulo AFD di rilevamento frodi attraverso la profilazione dell'autenticazione degli utenti.

IAP800® è rilasciabile nella versione ***On premise, Cloud e SaaS.***





Autenticazione per tutte le esigenze

READY FOR THE REAL WORLD

Principali Ambiti di utilizzo

Grandi bacini d'utenza

- ✓ *Strong Customer Authentication MFA* a servizi "mission critical" web e mobile, quali Home Banking, online Payments, online Fintech, online Insurance, neobanking, ecc.
- ✓ *Autenticazione Antifrode* contro qualsiasi Malware per Web e Mobile Banking
- ✓ *Firma Remota* nei servizi di Firma Digitale

Enterprise

- ✓ *Strong Authentication ai servizi Web aziendali (mediante web services)*
- ✓ *Strong Authentication alle reti aziendali LAN/WiFi (mediante radius, rest)*
- ✓ *Strong Authentication delle VPN aziendali*
- ✓ *Controllo Accessi e Rilevazione Presenze OTP*

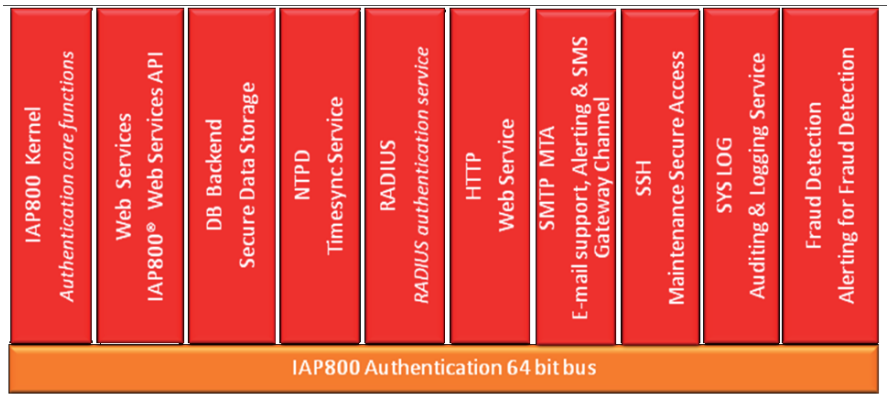
Small Medium Business

- ✓ *Strong Authentication in SaaS*
- ✓ *Strong Authentication in Cloud*

Motore di Autenticazione

L'ARCHITETTURA DI AUTENTICAZIONE

Come è realizzata



IAP800® Authentication Architecture

L'architettura dello IAP800® è modulare, costruita a partire dal *Kernel IAP800*, motore di autenticazione molto performante, in grado di gestire milioni di autenticazioni/ora, con risposte inferiori al secondo. Il Kernel è interconnesso agli altri moduli tramite bus a 64 bit.

Il modulo Web Services API permette una semplice integrazione con le Applicazioni Web, mentre quello RADIUS consente un'immediata integrazione con le risorse di rete.

L'HTTP Web Service ottimizza il dialogo con le applicazioni Web.

I moduli SMTP MTA sovrintendono ai servizi di rilascio otp tramite email ed sms.

La console amministrativa è disponibile tramite web / SSH.

I dati degli utenti e dei dispositivi sono registrati nel DB interno. Il monitoraggio e l'analisi delle attività del Server IAP800® sono affidati al SYS LOG e al Fraud Detection.

EASY Deployment & Easy Integration

EASY DEPLOYMENT

Semplice ed efficace

APPLIANCE Fisica/Virtuale on premise

IAP800® Server è disponibile sia come appliance fisica che come macchina virtuale VMware L'installazione e la configurazione dell'infrastruttura di autenticazione IAP800® è semplice ed efficace: definite le necessità, si possono agevolmente installare istanze singole o multi-active. Completa l'installazione, l'attivazione opzionale del modulo gateway IAP800GW per la gestione delle autenticazioni mobile M800.

CLOUD

Lo IAP800® è disponibile anche in Cloud, garantendo al contempo scalabilità e disponibilità, senza richiedere alcuna gestione on premise l'infrastruttura. E' certamente la scelta ideale per le applicazioni online.

MODALITA' SAAS

(Software as a Service)

Nel caso in cui il Cliente non intenda preoccuparsi della gestione dell'infrastruttura di autenticazione, è rilasciabile la versione IAP800® SaaS. In tal caso, tutto il servizio è amministrato da IRETH.

EASY INTEGRATION

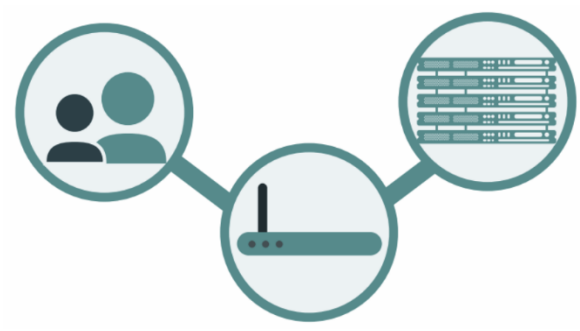
Immediata, attraverso protocolli standard come i Web Services basati su SOAP/XML o il RADIUS

SOAP/XML o RADIUS

L'integrazione del servizio di autenticazione forte e della profilazione dell'autenticazione (authentication fraud profiling) dello IAP800® nelle applicazioni o ambiente IT è immediata, attraverso l'implementazione dei protocolli standard:

- Web Services basato su SOAP/XML (per applicazioni web based)
- protocollo RADIUS (per l'accesso alla rete della vostra società, ecc.).

```
<?xml version="1.0" encoding=
<definitions name="AktienKurs
 targetNamespace="http://loc
 xmlns:xsd="http://schemas.xmlsoap.or
 xmlns="http://schemas.xmlsoap.org/ws
 <service name="AktienKurs">
  <port name="AktienSoapPort" binding
   <soap:address location="http://loc
  </port>
  <message name="Aktie.HoleWert">
   <part name="body" element="xsd:Tra
  </message>
  …
 </service>
</definitions>
```



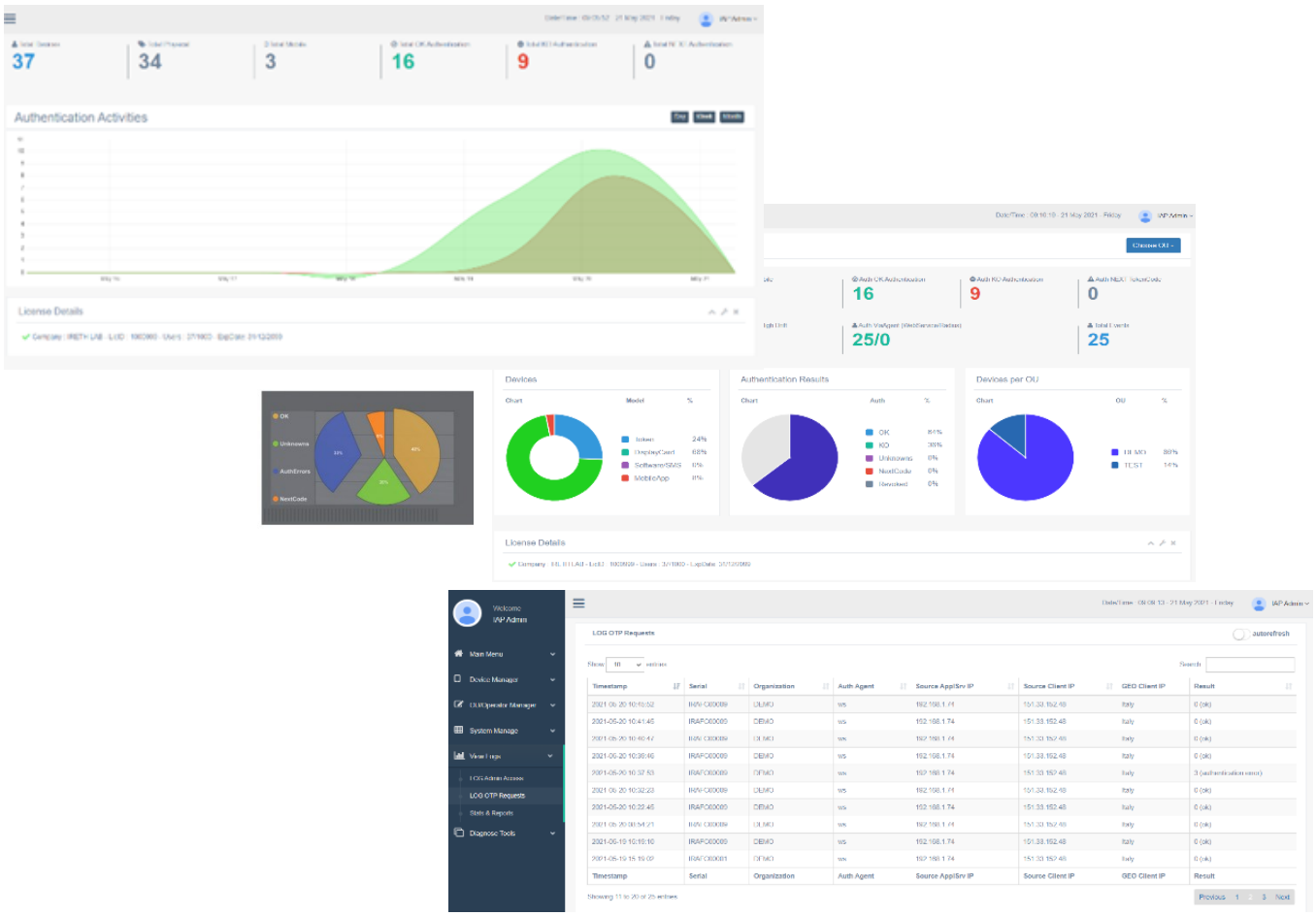
Easy to use & admin

PER L'UTENTE

L'autenticazione per l'utente è immediata e semplice da effettuare, qualsiasi sia il dispositivo messo a disposizione da IRETH per ogni esigenza: Token, Displaycard, Mobile App, Smartcard antifrode, Dynamic CVV, OTP via SMS garantiscono tutti affidabilità e sicurezza.

PER L'AMMINISTRATORE

La gestione dello IAP800 è semplice, grazie ad una GUI web-based completa, funzionale e dotata di reportistica. La gestione del server IAP800 può essere effettuata anche tramite console sfruttando i Web Services disponibili, la cui flessibilità permette di gestire agevolmente grandi bacini di utenza.



Caratteristiche principali IAP800 Server

IAP800® Server - CARATTERISTICHE PRINCIPALI

Motore Autenticazione	OATH FIDO
Algoritmi	HOTP, TOTP, OCRA-1 (OATH) RCR, CRT, AFT (IRETH) FIDO UAF, FIDO2
Moduli	Anti Frode, gestione carte AFC800 Integrità Transazionale Rilevamento Frodi Analysis & Logging delle Richieste OTP MAPM Multi Authentication Provider Manager
Integrazione	Web Service, LDAP e Radius per l'accesso alla rete societaria
Interoperabilità	In ambienti con due o più Provider OTP, il Server IAP800, attraverso il suo Modulo MAPM, offre una soluzione semplice e interoperabile per gestire differenti sistemi di autenticazione (OATH, FIDO). Il Modulo MAPM gestisce e indirizza tutte le richieste di autenticazione al corretto provider
Console	Intuitiva, professionale, anche tramite GUI
Standard	OATH FIDO PSD2 GDPR
Performance	2.500 autenticazioni/sec per appliance (→ più di 5 milioni di utenti ad appliance)
Canali	Multi-Canale: Internet / Mobile / Telefono
Gestione	Zero Gestione in Server-Farm (Versioni: Appliance o Virtual-Server appliance)
Sicurezza	Supporto completo in Alta Affidabilità (Multi Active) Supporto infrastruttura di Disaster Recovery
Supporto	SLA, sino a 24/7 Supporto Infrastrutturale in caso di Disaster Recovery

SUITE DI DISPOSITIVI OATH

Dispositivi di Autenticazione Forte per ogni esigenza

Portafoglio Dispositivi d'utenza

M800™ ed M800 Plus Mobile App, sono App token per Android e iOS, rilasciabili con funzionalità di sola Autenticazione (M800) o Autenticazione & Antifrode (M800 Plus) insieme ai dispositivi della suite AFC800™**;** le M800™App sono adatte a servire grandi bacini d'utenza e sono prontamente utilizzabili scaricandole dai vari store a seguito della registrazione al servizio IAP800.

android

iOS

M800
Authentication

M800 Plus
Authentication & Antifraud

T800™ Token suite: d'uso immediato ed economici, sono impiegati prevalentemente nei servizi rivolti ad un grande bacino d'utenza, presentando il minor Total Cost of Ownership. Sono rilasciabili con algoritmi OATH HOTP/TOTP/OCRA-1 e crittografia HMAC-SHA-1 o HMAC-SHA-256. Le versioni CR, con algoritmo Challenge-Response OCRA-1, sono idonee ad impieghi di Banking PSD2, dynamic linking

T804

T801

T803

T806-CR PSD2

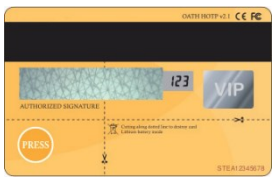
D800™ Displaycard suite: portabili e facili da usare, sono impiegate sia in ambito enterprise, per gli accessi 2FA ai servizi aziendali (anche insieme al servizio IAP800 SaaS o a IAP800 Cloud), che in ambito B2C, nei servizi per grandi bacini d'utenza . Sono rilasciabili con algoritmi OATH TOTP/HOTP/OCRA-1 e crittografia HMAC-SHA-1 o HMAC-SHA-256. Le versioni CR con algoritmo Challenge-Response OCRA-1 sono idonee ad impieghi di Banking PSD2, dynamic linking. Completano la suite i modelli EMV di pagamento nelle versioni CR e DCVV Dynamic CVV per la protezione dalle frodi CNP Card-Not-Presence nei pagamenti online

D800-1K

D800-CR 13K

D800-CR-Ble

D800-CR 13K EMV



D800-DCVV EMV

DISPOSITIVI Antifrode per Mobile e Web

AFC800™ antifraud suite per la *completa protezione Antifrode dei servizi Mobile / Web banking.* AFC800 è rilasciabile nei seguenti formati:

AFC800 SOLO

AFC800 EMV card

AFC800 Cardlet License

AFC800 Virtual License

AFC800 può essere rilasciata:

→ nei formati smartcard "Solo" non EMV o EMV card (di nuova emissione)
→ attraverso la *Licenza AFC800 Cardlet, come software* CAP cardlet da installare nelle Java Card EMV (di nuova emissione)
→ *mediante Licenza AFC800 Virtual,* per EMV card già emesse, con attivazione funzionalità "AFC virtual" sul server IAP800

Tutti i formati richiedono l'integrazione delle funzionalità antifrode AFC800 sulle App di banking del Cliente, mediante l'**SDK M800 Plus** fornito dalla stessa IRETH

DISPOSITIVI FIDO

M800 FIDO Mobile App è un App token per Android e iOS, con funzionalità MFA *Multi Factor Authentication* passwordless. L'autenticazione avviene attraverso parametri biometrici con riconoscimento vocale / facciale / fingerprint

M800 FIDO è basata su un'infrastruttura a chiave pubblica (PKI). Ad ogni utente vengono assegnate due *key*, quella pubblica registrata sul server e quella privata memorizzata sullo smartphone.

Semplicità d'uso	Funzionamento rapido ed intuitivo. Nessuna necessità di digitare credenziali ne password
Privacy e Sicurezza	Basata su una PKI, che garantisce l'integrità e non ripudiabilità
Firma della transazione	Attraverso il protocollo di autenticazione challenge-response

M800 – M800 Plus SDK

La **M800 SDK™** è una libreria di facile impiego per lo sviluppo di mobile App Token di autenticazione forte ai servizi web tramite lo standard OATH.

Caratteristiche Principali M800 SDK

- ✓ sviluppo semplificato e guidato di Mobile App Token OATH per Android e iOS
- ✓ standard OATH: TOTP / OCRA
- ✓ protezione contro gli di attacchi di "Phishing" e "Man-In-The-Middle"
- ✓ generazione di Mobile App Token correlata univocamente all'HW dello smartphone, con tracciamento dell'impronta dell'hardware stesso
- ✓ generazione del codice OTP non clonabile
- ✓ generazione dei codici OTP con cifratura dei dati SHA1 o SHA256 e mutua autenticazione con il server IAP800®
- ✓ disponibilità di un Vault cifrato ad uso dello sviluppatore per archiviare ulteriori dati sensibili
- ✓ generazione token contro tentativi di reverse engineering o di cracking del codice stesso

Caratteristiche Principali M800 Plus SDK

- ✓ tutte le caratteristiche della M800 SDK
- ✓ integrazione funzionalità Antifrode AFC800

M800 SDK android iOS

OVERVIEW DISPOSITIVI

	DISPLAYCARD	TOKEN	MOBILE TOKEN APP	AFC800	SMS OTP	DCVV
Caratteristiche	Facile da usare Portabile Resistente Antifrode (OCRA)	Facile da usare Economico Resistente Antifrode (OCRA)	Basato su Software No cost per l'utente Elevati costi per il gestore No Antifrode, senza AFC800	Uso immediato Portabile Low Cost Antifrode	Nessun software e nessun hardware No cost per l'utente	Facile da usare Portabile Resistente Antifrode -CNP
Target di Utenti	Corporate Consumer	Consumer Corporate	Consumer	Consumer Corporate	Consumer Corporate	Consumer
Algoritmi Supportati	OATH HOTP OATH TOTP OATH OCRA	OATH HOTP OATH TOTP OATH OCRA	OATH HOTP OATH TOTP OATH OCRA FIDO	OATH HOTP OATH TOTP OATH OCRA PKI	OATH TOTP	OATH TOTP (Time based)
Durata della Batteria	3 anni	3 anni	-	No battery	-	5 anni
Certificazioni	OATH ISO 7810 ISO 7816 ISO 1443 PSD2 GDPR RoHS	OATH PSD2 GDPR RoHS	OATH PSD2 FIDO	OATH EMV PSD2 ISO7810 ISO7816 GDPR RoHS	OATH	OATH EMV ISO7816 RoHS

Torino
Via A. Genovesi, 19 – 10128
Tel. +39 011 5089293

Milano
Via Fabio Filzi, 27 - 20124
Tel. +39 02 80886507

Villaverla (VI)
Via Capovilla, 73 – 36030
Tel. +39 0445 350464

info@ireth.net | www.ireth.net

info@iap800.com | www.iap800.com