Un modello di riferimento per la sicurezza degli *e-payments* alla luce del contesto di business e normativo emergente

Ing. Andrea Agosti
Responsabile Servizio Security (BU Sicurezza, Rischi e Compliance ICT)

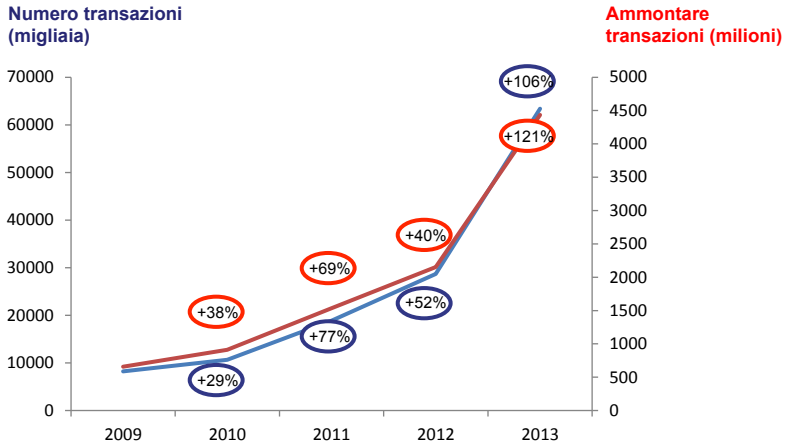
SPIN 2014 – 24 Giugno 2014, Centro Congressi Porto Antico di Genova

Agenda dell'intervento

- ***Premessa: il contesto di riferimento in tema di e-payments, cybersecurity ed e-identity***
- Un modello di riferimento per la sicurezza di un sistema di e-payments
- Raccomandazioni per banche / PSP in tema di sicurezza dei servizi di e-payments
- Il posizionamento di Oasi S.p.A. e del Gruppo ICBPI in materia di sicurezza degli e-payments.

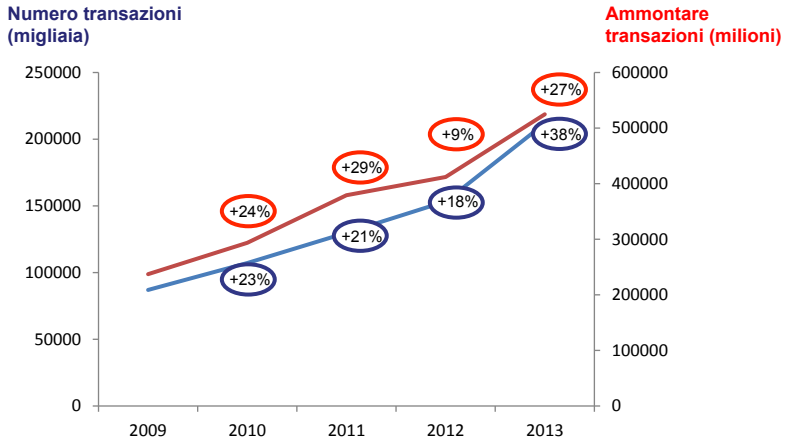
L'adozione e la diffusione di strumenti e servizi di *e-payments* per effettuare pagamenti tramite Internet è un trend in continua crescita

Pagamenti tramite carte di credito in rete



Fonte: elaborazione OASI su dati ABI, I sistemi di pagamento nella realtà italiana, Dic 2013

Pagamenti tramite bonifici in rete



Fonte: elaborazione OASI su dati ABI, I sistemi di pagamento nella realtà italiana, Giu 2012 e Dic 2013

On line / mobile payment service provider

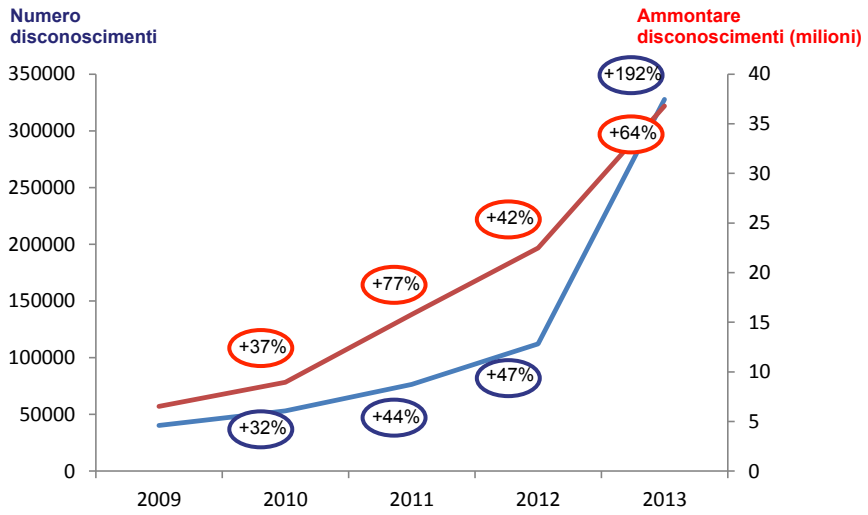
PayPal
Google wallet
amazonpayments
Authorize.Net
DWOLLA
Pingit
2CO 2CHECKOUT.COM
stripe
Braintree
WePAY

Considerazioni chiave

- Incremento esponenziale dell'utilizzo delle carte di credito in rete (2013 / 2012, +106% in volume transazioni e + 121% in ammontare transazioni)
- Forte incremento dell'utilizzo della rete per l'esecuzione di disposizioni di bonifico (2013 / 2012, +38% in volume transazioni e +27% in ammontare transazioni)
- Nascita di numerosi On line / mobile payment service provider non sempre legati direttamente a realtà bancarie

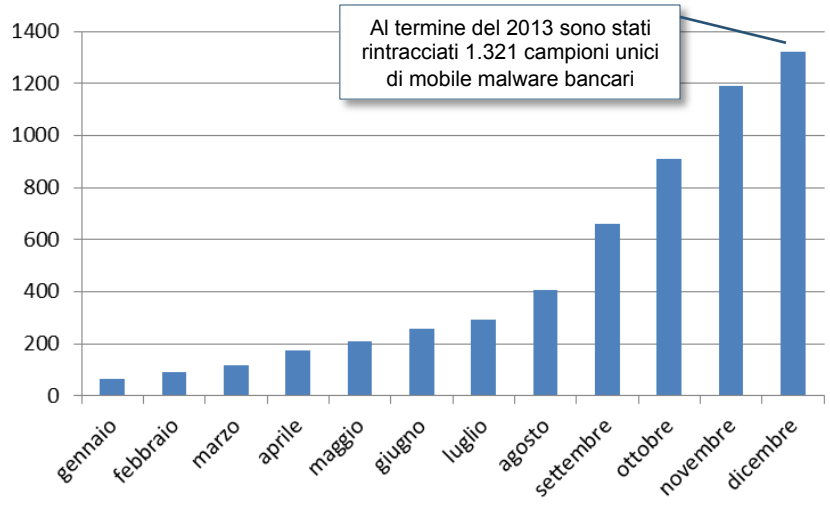
La sicurezza rappresenta ancora uno dei principali problemi legati ad una più ampia accettazione di strumenti e servizi di *e-payments*

Transazioni non riconosciute (Card Not Present)



Fonte: elaborazione OASI su dati UCAMP 2014

Diffusione di mobile malware bancari nel 2013



Fonte: elaborazione OASI su dati Kaspersky Lab – febbraio 2014

Esiti dal rapporto sulle frodi informatiche ABILab 2104

- Il mondo bancario rappresenta ancora uno dei target principali dei cybercriminali e la continua sofisticazione degli attacchi informatici via Internet e Mobile Banking, richiede un continuo monitoraggio e presidio dei fenomeni
- Si è registrato un aumento dell'efficacia dei casi di phishing e dei relativi volumi economici interessati
- Particolare interesse si sta diffondendo sul tema della sicurezza dell'identità digitale, anche nell'ottica di un incremento dei processi di vendita on line

Considerazioni chiave

- La diffusione dei malware dedicati ai dispositivi mobile, sempre più utilizzati dalla clientela per eseguire operazioni di pagamento non sta mostrando segni di rallentamento, anche se il canale web continua a rappresentare la scelta preferenziale per i tentativi di frode informatica
- Durante il 2013 il numero delle modificazioni malware mobile disegnate per perpetrare il furto di dati di carte di credito e di denaro è aumentato di circa venti volte

La BCE è intervenuta di recente con una serie di «Raccomandazioni» relative alla sicurezza degli *e-payments*, in particolare in ambito Internet e Mobile

Raccomandazioni BCE

Principali contenuti

- La **BCE** ha pubblicato due documenti, uno recante disposizioni in tema di «*Sicurezza dei pagamenti effettuati via Internet*» (in versione definita) ed uno recante disposizioni in tema di «*Sicurezza sui pagamenti mobile*» (in consultazione)

- Le **raccomandazioni** sono suddivise in **3 macro-categorie** a seconda dei temi che indirizzano:
  - *General control and security environment*, per i temi di **governance**, **risk identification** / **assessment**, **monitoring** / **reporting**, **risk control** / **mitigation** e **tracciabilità**
  - *Specific control and security measures for Internet Payment / mobile payments*, per i temi di **accesso** ed **esecuzione** del servizio di pagamento, **autorizzazione** e **monitoraggio** delle transazioni e **protezione** delle **informazioni / quantità** di **sicurezza**
  - *Customer awareness, education and communications*, per i temi di **corretta informazione** e **sensibilizzazione** dei **clienti** sull'utilizzo sicuro dei servizi di pagamento

- Per le disposizioni in tema di «Sicurezza dei pagamenti effettuati via internet» *(richiamate anche dalle recenti disposizioni di Vigilanza)*, le **Banche** ed i **Prestatori** di **Servizi** di **Pagamento** dovranno adeguarsi alla normativa **entro** il **1 Febbraio 2015.** Con riferimento a quello in tema di «Sicurezza dei pagamenti mobile», invece, la data ultima entro la quale dovranno conformarsi gli operatori è ancora da definire – attualmente è il **1 Febbraio 2017**.

I° Pilastro delle Raccomandazioni BCE per la sicurezza degli *e-payments*: «*General control and security environment*»

Focus on: Sicurezza dei pagamenti effettuati via Internet

Ambito	Principali requisiti
Governance	– Deve essere predisposta una policy di sicurezza, rivista con cadenza regolare e approvata dal senior management – La policy deve definire ruoli e responsabilità, incluse quelle del risk management
Risk assessment	– Deve essere effettuato con cadenza regolare – Sulla base delle risultanze delle attività di risk assessment devono essere identificati le modifiche da introdurre sulle misure di sicurezza esistenti - I risk assessment devono prevedere la revisione degli scenari di rischio e delle misure di sicurezza a seguito di incidenti di sicurezza rilevanti, in caso di cambiamenti significativi del contesto tecnologico di riferimento, a seguito dell'identificazione di nuove minacce
Incident monitoring and reporting	- Deve essere implementato un processo per il monitoraggio, la gestione e la consuntivazione degli incidenti di sicurezza e la relativa segnalazione al management e deve essere definita una procedura per la notifica immediata degli incidenti di maggiore rilevanza alle Autorità Competenti - Deve essere definite una procedura di collaborazione con le Agenzie competenti in caso di incidenti di sicurezza rilevanti, inclusi casi di furto di dati critici - I Prestatori di Servizi di Pagamento che svolgono attività di acquiring devono obbligare contrattualmente gli e-merchant che gestiscono / custodiscono dati critici a cooperare in caso di accadimento di incidenti rilevanti
Risk control and mitigation	- Devono essere implementate misure di sicurezza secondo standard / best practice di sicurezza (SoD, Least privilege, …) - Devono essere previsti processi di monitoraggio, tracciatura e restrizione degli accessi ai dati critici e alle risorse logiche e fisiche coinvolte e devono essere idonee soluzioni di tracciatura - Deve essere seguito il principio della «data minimization» per tutte le attività di gestione dei dati critici (raccolta, elaborazione, storicizzazione, …) - Le misure di sicurezza devono essere testate sotto la supervisione della struttura di Risk Management per verificarne robustezza ed efficacia e devono essere previsti audit da parte di terze parti indipendenti (interne o esterne). - Laddove è previsto l'outsourcing di attività di sicurezza, deve essere richiesto a livello contrattuale il rispetto delle raccomandazioni definite nel documento ECB.
Traceability	- Devono essere previsti meccanismi per il tracciamento dettagliato delle transazioni e dei dati relativi agli e-mandate - Devono essere disponibili soluzioni per effettuare ricerca ed analisi sulle transazioni e sui dati relativi agli e-mandate - I Prestatori di Servizi di Pagamento che svolgono attività di acquiring devono obbligare contrattualmente gli e-merchant che gestiscono / custodiscono dati critici ad adeguare i relativi processi interni per supportare la tracciabilità delle transazioni e dei flussi relativi agli e-mandate

II° Pilastro delle Raccomandazioni BCE per la sicurezza degli *e-payments*: «*Specific control and security measures for e-payments*»

Focus on: Sicurezza dei pagamenti effettuati via Internet

Ambito	Principali requisiti
Initial customer identification, information	− Il Cliente deve essere adeguatamente riconosciuto, dal PSP in linea con le normative vigenti − Il PSP deve fornire informazioni preliminari al Cliente rispetto ai servizi di pagamento Internet, rispetto a strumenti e software forniti, modalità di utilizzo sicuro del servizio, processi di contatto con il PSP, etc. − Il PSP, nei contratti di servizio fatti stipulare dal Cliente, deve specificare che può bloccare transazioni / strumenti di pagamento per motivi di sicurezza − Il PSP deve fornire informazioni anche continuative su responsabilità nell'utilizzo sicuro del servizio
Strong customer authentication	− Deve essere effettuata l'autenticazione forte del Cliente, in accordo alla specifica definizione di strong authentication fornita dalle raccomandazioni, salvo le diverse eccezioni previste e dettagliate nel paragrafo − La strong authentication deve essere supportata / attiva anche in ambito carte di pagamento e in ambito wallet
Enrolment for and provision of auth. tools and/or sw delivered to the cust.	− La registrazione e la fornitura degli strumenti di autenticazione forte ed anche di eventuale software deve avvenire in conformità a specifici requisiti di sicurezza − I PSP issuer devono incoraggiare l'utilizzo dell'autenticazione forte da parte dei clienti, non richiedendola solo in caso di transazioni a basso rischio
Log-in attempts, session time out, validity of authentication	− Devono essere previsti limiti temporali di validità password (il minimo indispensabile) − Deve essere previsto un numero massimo di tentativi di accesso e implementati meccanismi di blocco account − Deve essere previsto un tempo massimo di validità della sessione
Transaction monitoring and authorisation	− Deve essere attive soluzioni di transaction monitoring delle transazioni che ne permettano il blocco prima dell'esecuzione. Devono essere attive soluzioni per rilevazione connessioni potenzialmente anomale, indice di infezione da malware − La complessità dei sistemi deve essere commisurata al rischio − Gli acquirers devono avere soluzioni di prevenzione frodi per monitorare attività dei merchant − Le analisi rispetto alle transazioni bloccate devono essere svolte in tempi congrui e − I blocchi dovrebbero essere mantenuti per il minimo necessario
Protection of sensitive payment data	− Tutti i dati usati per identificare e autenticare i Clienti devono essere sicurizzati contro il furto e l'accesso non autorizzato o la modifica − Per lo scambio dei dati via internet, devono essere utilizzate soluzioni di crittografia conosciute − I PSP che offrono servizi di acquiring devono incoraggiare i loro e-merchant a non salvare qualsiasi dato sensibile di pagamento

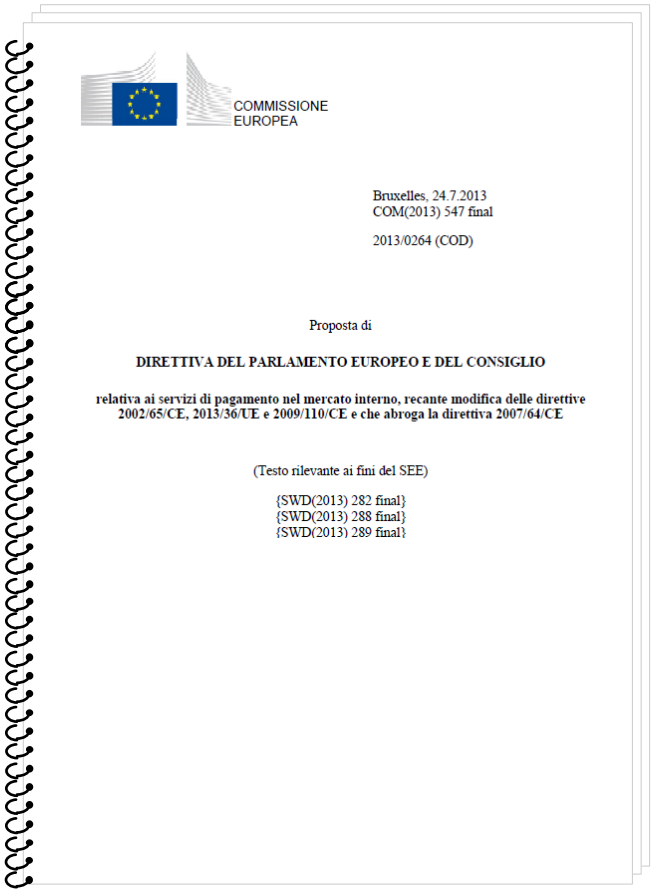
III° Pilastro delle Raccomandazioni BCE per la sicurezza degli *e-payments*: «*Customer awareness, education and communication*»

Focus on: Sicurezza dei pagamenti effettuati via Internet

Ambito	Principali requisiti
Customer education and communication	- Deve essere previsto l'utilizzo di almeno un canale sicuro (mail box dedicata su sito del PSP o sito PSP sicuro) o per le comunicazioni con la clientela relative alle modalità di utilizzo sicurezza dei servizi. I PSP devono utilizzare tale canale e informare il cliente che le comunicazioni che utilizzano altri mezzi devono essere considerate non affidabili. Il PSP deve comunicare la procedura con cui comunicare al PSP casi di frode (anche sospetta), sospetti di incidenti o di anomalie, le azioni conseguenti (e.g. modalità di risposta del PSP) e le modalità con cui il PSP informa il cliente rispetto a potenziali frodi o a casi di attacco - Tramite il canale sicuro il PSP deve tenere informato i clienti rispetto ad aggiornamenti delle procedure di sicurezza e fornire segnalazioni rispetto a rischi emergenti - Il PSP deve rendere disponibile assistenza alla clientela per richieste e supporto relative ai servizi erogati e il cliente deve essere informato su come può richiedere tale assistenza - I PSP e, dove rilevante, le Autorità di Controllo devono sviluppate iniziative di formazione della clientela che garantiscano la conoscenza almeno dei seguenti temi • Protezione delle password, dei token di sicurezza, delle informazioni personali e dei dati critici • Gestione dei dispositivi personali (e.g computer) tramite l'installazione di componenti di sicurezza aggiornati (e.g. antivirus, firewall, patches, …) • Minacce e rischi derivanti dal download di software via internet, nel caso in cui il cliente non sia ragionevolmente certo della provenienza e della relativa integrità • Utilizzo del sito internet effettivo del PSP per i pagamenti - I PSP che operano come acquirer devono chiedere agli e-merchant di distinguere il sito in cui viene effettuato l'acquisto da quello in cui viene perfezionato il pagamento, ad esempio tramite re-indirizzamento e apertura di altre finestre operative - I PSP che operano come acquirer devono sviluppare programmi di formazione per i relativi e-merchant su tematiche di fraud mgmt*
Notifications, setting of limits	- Prima di attivare il servizio, il PSP deve definire limiti operativi per il cliente (e.g. massimale per operazione e massimale per periodo) che ne deve essere informato. Il PSP deve consentire al cliente di disattivare i servizi di pagamento via internet
Customer access to information on the status of payment initiation and execution	- I PSP devono fornire servizi in tempo «quasi reale» per verificare lo stato di esecuzione delle transazioni così come il saldo delle operazioni in un ambiente sicuro e verificato - Il dettaglio delle operazioni deve essere disponibile in formato elettronico in un ambiente sicuro e verificato. Laddove siano utilizzati canali alternativi di informazione (SMS, mail, lettere, …) non devono essere trasmessi dati critici oppure questi devono essere mascherati

La revisione della Payment Services Directive (cd PSD II) prevede misure ancora più significative per il contrasto alle frodi sui sistemi di pagamento

PSD II *(doc. in consultazione)*



COMMISSIONE EUROPEA

Bruxelles, 24.7.2013
COM(2013) 547 final

2013/0264 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 2002/65/CE, 2013/36/UE e 2009/110/CE e che abroga la direttiva 2007/64/CE

(Testo rilevante ai fini del SEE)

{SWD(2013) 282 final}
{SWD(2013) 288 final}
{SWD(2013) 289 final}

Principali indicazioni in tema di sicurezza

Art. 5 – Domanda di autorizzazione

L'autorizzazione a svolgere attività come istituto di pagamento è subordinata alla presentazione alle autorità competenti dello Stato membro d'origine di una domanda corredata dalle informazioni seguenti […]:
(j) un documento relativo alla politica di sicurezza, una valutazione dettagliata dei rischi relativi ai servizi di pagamento offerti e una descrizione delle misure di controllo e di mitigazione adottate per tutelare adeguatamente gli utenti contro i rischi individuati in materia di sicurezza, compresi la frode e l'uso illegale di dati sensibili e personali

Art. 66 – Responsabilità del pagatore per le operazioni di pagamento non autorizzate

[…] Per i pagamenti eseguiti tramite una tecnica di comunicazione a distanza, se il prestatore di servizi di pagamento non esige una autenticazione a due fattori del cliente, il pagatore non sopporta alcuna conseguenza finanziaria salvo qualora abbia agito in modo fraudolento. Qualora non accettino un'autenticazione a due fattori del cliente, il beneficiario o il suo prestatore di servizi di pagamento rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore.

Art. 87 – Autenticazione

1. Gli stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione a due fattori del cliente quando il pagatore dispone un'operazione di pagamento elettronico, salvo deroghe specifiche previste dagli orientamenti dell'ABE sulla base del rischio connesso al servizio di pagamento prestato. […]

3. In stretta cooperazione con la BCE, l'ABE emana orientamenti indirizzati ai prestatori di servizi di pagamento riguardanti le tecniche più avanzate di autenticazione del cliente e le eventuali deroghe all'uso dell'autenticazione a due fattori del cliente. […]

In Italia, il Sistema Pubblico per l'Identità Digitale (SPID) previsto dall'Agenzia per l'Italia Digitale offre opportunità alle Banche ed ai PSP (1 / 2)

Lo SPID rappresenta l'infrastruttura nazionale di autenticazione dei cittadini italiani prevista per l'accesso a servizi on-line della pubblica amministrazione e privati. Attraverso un modello federato di gestione dell'identità digitale ed interoperabile su diversi canali, risponde all'esigenza di mettere a fattor comune un sistema di autenticazione certa: chiunque gestisca un servizio, potrà collegarsi e beneficiare di un sistema di gestione di credenziali, senza doverlo realizzare *ex novo*.

L'uso di *Identità Digitali* sicure permetterà di:

- **aumentare** la **fiducia** dei cittadini nei servizi Internet, ivi inclusi i sistemi di pagamento on-line;
- **facilitare** l'**accesso** ai servizi abilitando una serie di nuove funzionalità utili come *l'e-commerce*
- **contrastare fenomeni criminali** quali *Furto d'Identità ed «impersonificazione»*
- **aumentare** la **tutela** della ***Privacy***, con la riduzione degli archivi contenenti dati personali.

L'avvio entro aprile 2015 del sistema SPID è una delle priorità indicate dal Presidente del Consiglio dei Ministri

Principali prescrizioni del Codice dell'Amministrazione Digitale (CAD)

- Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è **istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale** di cittadini e imprese (SPID)
- Il sistema SPID è **costituito come insieme aperto di soggetti pubblici e privati** che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, gestiscono i servizi di **registrazione e di messa a disposizione delle credenziali** e degli strumenti di accesso in rete nei riguardi di cittadini e imprese
- È altresì riconosciuta alle imprese la facoltà di avvalersi del sistema SPID per la **gestione dell'identità digitale dei propri utenti**
- Attraverso un apposito DPCM, previsto per luglio, verranno definite le caratteristiche del sistema SPID. Tra le caratteristiche che il DPCM dovrà specificare vi saranno in particolare:
  a) il modello architetturale e organizzativo del sistema;
  b) le modalità e i requisiti necessari per l'accreditamento dei gestori dell'identità digitale;
  c) gli standard tecnologici e le soluzioni tecniche e organizzative da adottare;
  d) le modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;
  e) le modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete

In Italia, il Sistema Pubblico per l'Identità Digitale (SPID) previsto dall'Agenzia per l'Italia Digitale offre opportunità alle Banche ed ai PSP (2 / 2)

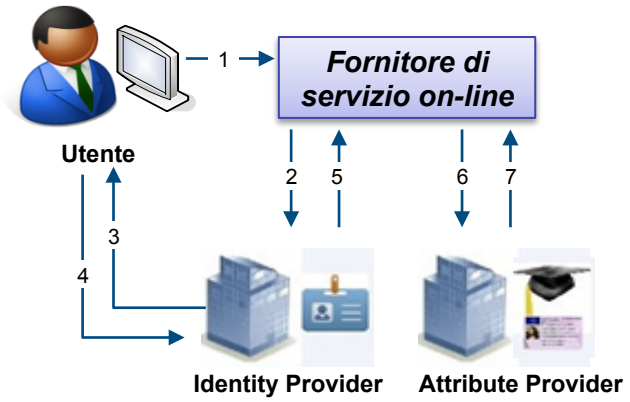
Lo SPID non introduce una nuova Identità Digitale, ma un protocollo sicuro avente come obiettivo principale l'interoperabilità delle credenziali e degli strumenti di accesso

Sono previsti tre differenti livelli di sistemi di autenticazione (Standard ISO/IEC 29115 :2013)

a) autenticazione a singolo fattore, come ad esempio la password.
b) autenticazione a due fattori, come ad esempio le One Time Password generate da dispositivi token
c) autenticazione a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi sicuri quali ad esempio le Smart Cart e le SecureSIM

L'Agenzia valuta e autorizza l'uso degli strumenti di autenticazione per ciascun livello, nonché l'assegnazione dei sistemi al relativo livello di sicurezza.

1. Richiesta di un servizio da parte di un utente (ad es. servizio di e-commerce)
2. Inoltro notifica della richiesta di accesso al «fornitore» delle Identità (ad es. Banca)
3. L'Identity Provider richiede le credenziali all'utente in base alle proprie tecnologie di autenticazione
4. L'utente inserisce le credenziali che vengono verificate dall'identity provider
5. In caso di riscontro positivo l'identity provider invia al service provider un'asserzione di avvenuta autenticazione e l'utente accede al servizio
6. Per orientare correttamente il servizio può essere necessario conoscere attributi aggiuntivi (età, provincia di residenza, appartenenza ad ordini professionali) chiesti all'Attrib. provider
7. L'A.P. fornisce le informazioni riferite all'utente distinte in tre categorie: Identificativi (nome, cognome..), non identificativi (es. consenso privacy), qualificati (abilitazioni professionali...)



Casi di successo di progetti nazionali di *e-Identity* che sono stati presi in considerazione per l''ideazione del Sistema Pubblico per l'Identità Digitale

L'Estonia è uno dei primi paesi al mondo per innovazione diffusione ed utilizzo delle nuove tecnologie Internet ed e-commerce.

- Già nel 2011 il 94% delle dichiarazioni dei redditi è stato compilato e presentato on line (sistema E-Tax), previa registrazione e autenticazione del contribuente, con un tempo medio richiesto di 5 minuti
- Il 25% dei voti nelle elezioni politiche del 2011 è stato espresso on line, così come il 62% delle risposte all'ultimo censimento (2012)

La National Strategy for Trusted Identities in Cyberspace è un'iniziativa del governo degli Stati Uniti, avviata nell'aprile 2011 per migliorare la protezione della privacy, la sicurezza e la fiducia nelle transazioni on-line ritenute sensibili, attraverso sforzi di collaborazione congiunta tra settore privato, le associazioni dei consumatori e le agenzie governative

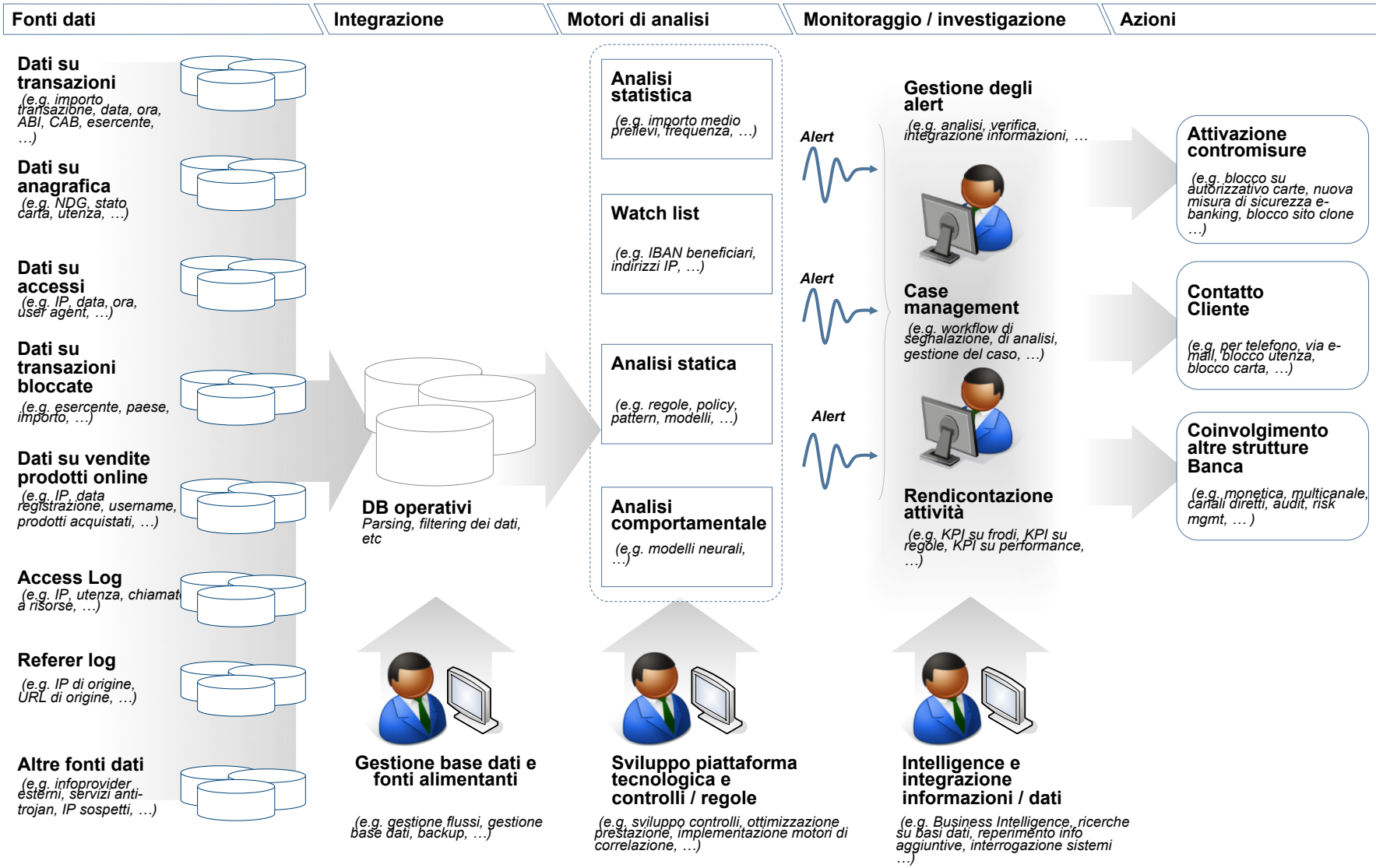
ASAN IMZA (Easy firma), istituito in Azerbaijan dal Ministero delle Imposte, in collaborazione con Ministero delle Comunicazioni e delle Tecnologie, è il servizio che permette ad un cittadino di utilizzare un telefono cellulare come una forma di sicura identità elettronica

BankID in Svezia rappresenta un servizio di identificazione elettronica, sviluppato attraverso la partecipazione delle maggiori banche nazionali. Più di 5 milioni di cittadini ricorrono al servizio di Identity Provider BankID per poter fruire di servizi offerti sia dal settore pubblico, sia dal settore privato

Agenda dell'intervento

- Premessa: il contesto di riferimento in tema di e-payments, cybersecurity ed e-identity
- ***Un modello di riferimento per la sicurezza di un sistema di e-payments***
- Raccomandazioni per banche / PSP in tema di sicurezza dei servizi di e-payments
- Il posizionamento di Oasi S.p.A. e del Gruppo ICBPI in materia di sicurezza degli e-payments.

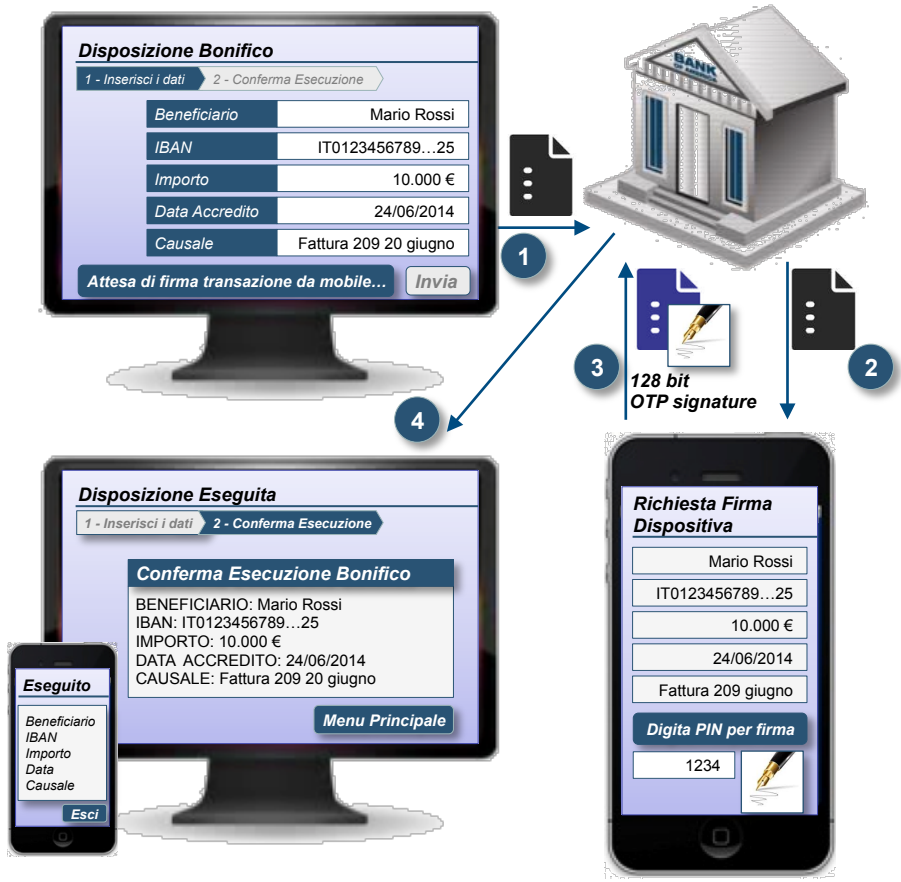
Modello logico di riferimento per l'architettura di un sistema di sicurezza finalizzato alla prevenzione e al contrasto alle frodi sugli e-payments



Focus on\1: soluzioni di *Strong Authentication* basate su algoritmi di *Transaction Data Signing* utilizzabili in ambiente *mobile*

Le attuali tecnologie di sicurezza permettono ai clienti di applicare alla transazione di pagamento, una firma digitale, basata su autenticazione a due fattori (*strong authentication*) che aumenta il livello di consapevolezza dell'utilizzatore riguardo alla disposizione che sta eseguendo e riduce il rischio frode per sofisticazione dei dati in transito tra dispositivo del Cliente e Servizio di Pagamento Elettronico da parte di attacchi informatici

1 ***Inserimento dati caratteristici della transazione***	Il Cliente compila il form di inserimento dati di pagamento elettronico (es. Bonifico bancario)
2 ***Controllo dati e conferma transazione***	I sistemi di sicurezza del payment service provider inviano i dati relativi alla transazione sul dispositivo mobile del Cliente in formato cifrato
3 ***OTP transazionale come firma dell'operazione***	Il Cliente controlla i dati dell'operazione, inserisce un PIN per confermare (opzionale) e la App trasmette una OTP di 128 bit contenente l'intero set di dati della transazione
4 ***Rendiconto dell'operazione eseguita***	Il Cliente visualizza il rendiconto dell'avvenuta operazione sia sul PC sia sulla App installata sul dispositivo mobile



In caso di utilizzo del solo canale mobile anche i punti 1 e 4 sono eseguiti attraverso la App installata sul dispositivo

Focus on\2: soluzioni di *Strong Authentication* basate su misure di riconoscimento biometrico di tipo fisico e comportamentale

La Strong Customer Authentication(1) consiste in una procedura di riconoscimento del Cliente basata sull'utilizzo congiunto di due o più fattori di verifica dell'identità, categorizzati come elementi che provano la conoscenza di un'informazione nota solo al cliente legittimo (password, PIN, codici di matricola identificativi…), il possesso di un oggetto (token di generazione One Time Password, smart card, dispositivo mobile…) e il possesso di caratteristiche intrinseche del cliente (dati biometrici fisici, dati biometrici comportamentali)

Posizionamento del settore finanziario

- Nel settore finanziario al fine di prevenire fenomeni fraudolenti per furto di identità, si assiste da diversi anni ad un largo utilizzo dei primi due fattori di autenticazione: *something only the user knows, something only the user possesses.*
- La diffusione dei dispositivi mobile smartphone sta favorendo una forte accelerazione nella ricerca e nella produzione di tecnologie di riconoscimento biometrico, che il settore finanziario sta valutando con interesse crescente, per offrire alla propria clientela soluzioni di autenticazione innovative, di semplice utilizzo, differenzianti rispetto ai competitor e che contribuiscono ad un positivo ritorno di immagine per l'intermediario
- Il Garante della Privacy ha sottoposto a consultazione pubblica il documento *Linee guida in materia di riconoscimento biometrico e firma grafometrica*

Smartphone con funzionalità di riconoscimento biometrico

- Dotato di interfaccia semplice, completa e ad Elevate prestazioni (accuratezza/efficienza)
- Portabilità e disponibilità costante per il cliente
- Costo contenuto
- Ingombro ridotto
- Elevata diffusione sul mercato

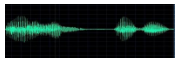
Elementi valutati nella scelta di una tecnologia biometrica

- Facilità d'uso - combinazione dispositivo-servizio
- Gradimento da parte della Clientela
- Incidenza di disturbi nel processo di riconoscimento
- Precisione offerta dalla tecnologia
- Livello di sicurezza richiesto
- Stabilità a lungo termine del fattore di autenticazione

Dati biometrici potenzialmente utilizzabili per rafforzare il livello di precisione nelle procedure di riconoscimento della clientela e-payments

Impronta digitale

Riconoscimento facciale



Riconoscimento Vocale

Firma Grafometrica

Riconoscimento dell'iride

Confronto con pattern comportamentale riguardante l'interazione cliente – sito web (battitura, movimentazione del mouse, scroll delle pagine,…) o cliente – dispositivo mobile (swipe, pressioni sul display, tasti più utilizzati, dati del giroscopio, errori di battitura,…)

Behavioral biometric measures

(1) *Definizione formalizzata nelle Recommendations for the security of internet payments - European Central Bank*
(2) *www.garanteprivacy.it, doc. web n. 3127397*

Focus on\3: soluzioni di Adaptive Authentication e Transaction Monitoring per il monitoraggio delle caratteristiche di rischio associate alle transazioni

In linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati su Internet, a complemento delle misure di prevenzione frode basate su strong customer authentication, ricoprono un ruolo chiave le soluzioni di monitoraggio delle transazioni e di analisi comportamentale della Clientela, utili a riscontrare possibili anomalie sulla base di valutazioni di rischio, che non possono essere rilevate con la sola applicazione di controllo accessi a più fattori di autenticazione

Adaptive Authentication

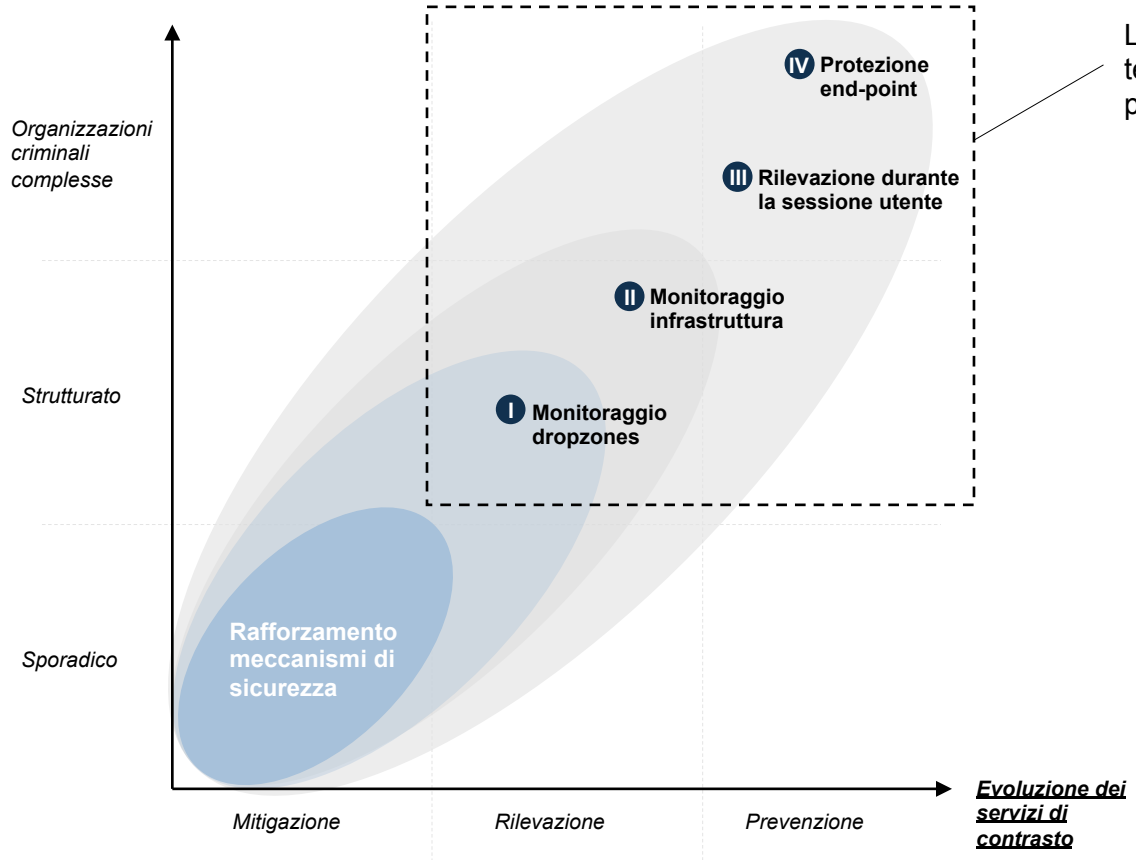
- È una tecnologia che adatta il metodo di autenticazione da proporre al Cliente in base al rischio calcolato in funzione di una serie di parametri deterministici, legati al dispositivo con cui ci si collega al servizio, e probabilistici, legati al profilo comportamentale del Cliente
- Ricorre a profilazione comportamentale, processo in cui i tipici schemi di utilizzo del servizio seguiti dal Cliente sono utilizzati per distinguerlo da un utente non autorizzato
- Basa le valutazioni di rischio anche sulla profilazione di dispositivo, processo in cui le caratteristiche intrinseche del pc, laptop, dispositivo mobile, sono utilizzate per distinguere un Cliente leggittimo da un utente non autorizzato
- L'analisi di rischio è effettuata durante la fase di accesso al servizio di pagamento, per modulare il livello di «challenge» verso l'utente, ad esempio:
  - Rischio basso per parametri di connessione tipici ed accesso in consultazione a dati non utilizzabili per condurre frodi
    - Sufficiente la sola verifica della password
  - Rischio medio per accesso in orario inusuale per il Cliente o per parametri di connessione diversi dal solito
    - Strong Customer Authentication
  - Rischio elevato, quasi tutti i fattori di valutazione sono disallineati dal pattern usuale
    - Accesso momentaneamente negato o chiamata di verifica al Cliente

Transaction Monitoring

- La soluzione è volta a prevenire, rilevare e bloccare le transazioni di pagamento fraudolente prima dell'autorizzazione finale del Payment Service Provider
- Le transazioni sospette o ad alto rischio vengono poste in evidenza e sottoposte ad uno screening specifico e ad una procedura di valutazione
- L'analisi di rischio è effettuata durante la fase di navigazione nell'area riservata del Servizio, a valle del passo di autenticazione, per segnalare eventuali anomalie comportamentali dell'utente
  - Improvviso cambio dei parametri di connessione, indice di un possibile attacco informatico
  - Utilizzo del servizio in orari inusuali per il Cliente
  - Velocità di navigazione differente dai casi precedenti
  - Ordine delle pagine navigate mai seguito
  - Importi delle transazioni di valore inconsueto
  - Frequenza di disposizione delle transazioni
  - Incompatibilità geografica

Focus on\4: i servizi di prevenzione e contrasto delle minacce *online* di furto delle credenziali per l'autenticazione dei servizi di *e-payments*

La continua evoluzione del fenomeno e delle varianti di malware, nonché la maggior facilità con la quale anche individui non dotati di skills tecniche riescono ad accedere e ad utilizzare vere e proprie "suite" di software malevolo, rendono necessaria l'implementazione di contromisure che possano **non solo rilevare** evidenze ex-post rispetto all'infezione da malware, ma **prevenire l'infezione stessa e i danni causati dal malware**. Le misure sotto riportate non possono comunque prescindere dall'adozione di strumenti e servizi di *intelligence*, per la tempestiva identificazione ed analisi anche tecnica delle minacce che potrebbero mettere a rischio la sicurezza di soluzioni di sicurezza dell'Istituzione Finanziaria:



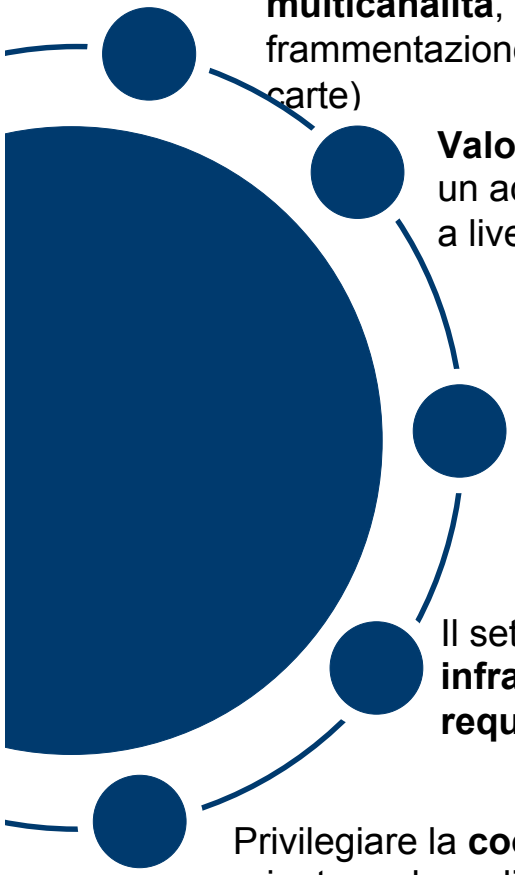
Le Istituzioni Finanziarie hanno, nel corso del tempo, implementato soluzioni via via più efficaci per la detection del fenomeno malware:

- **I** Individuazione dei dati carpiti ai Clienti delle istituzioni finanziarie, mediante monitoraggio delle dropzone dove sono inviate le credenziali ed eventuali altri dati sottratti
- **II** Rilevazione di eventuali connessioni anomale derivanti da comportamenti noti dei malware, mediante il monitoraggio dell'infrastruttura dell'istituzione finanziaria
- **III** Rilevazione, attraverso script eseguiti sul browser dell'utente, di software malevolo
- **IV** Protezione del device dell'utente mediante l'installazione di software di protezione dell'end-point – *soluzione ad elevato impatto per l'user experience dell'utente e di potenziale difficile applicabilità*

Agenda dell'intervento

- Premessa: il contesto di riferimento in tema di e-payments, cybersecurity ed e-identity
- Un modello di riferimento per la sicurezza di un sistema di e-payments
- ***Raccomandazioni per banche / PSP in tema di sicurezza dei servizi di e-payments***
- Il posizionamento di Oasi S.p.A. e del Gruppo ICBPI in materia di sicurezza degli e-payments

Conclusioni e raccomandazioni per banche / PSP in tema di modello operativo e architettura funzionale per il presidio della sicurezza degli *e-payments*



Affrontare le sfide poste dalla sicurezza e dal contrasto alle frodi in una logica di **multicanalità**, privilegiando il **cliente** al **centro** dell'**esperienza** ed evitando la frammentazione di dispositivi / prassi differenti sui vari canali (e.g. Internet, mobile, carte)

Valorizzare gli **investimenti** in strumenti di ***strong authentication*** mediante un adeguato posizionamento in materia di ***e-Identity***, sfruttando le opportunità a livello domestico (e.g. SPID) e comunitario (e.g. STORK 2.0)

Evitare la focalizzazione sul conseguimento di livelli di conformità al 100%, ma predisporre **architetture tecnologiche** e **modelli operativi** fondato su **logiche** di **gestione** del **rischio** delle frodi

Il settore dei pagamenti è ormai considerato a livello EU come una **infrastruttura critica** della ***Digital Society***, la **Cybersecurity** è un **requisito minimo** per potervi accedere ed operare nel tempo

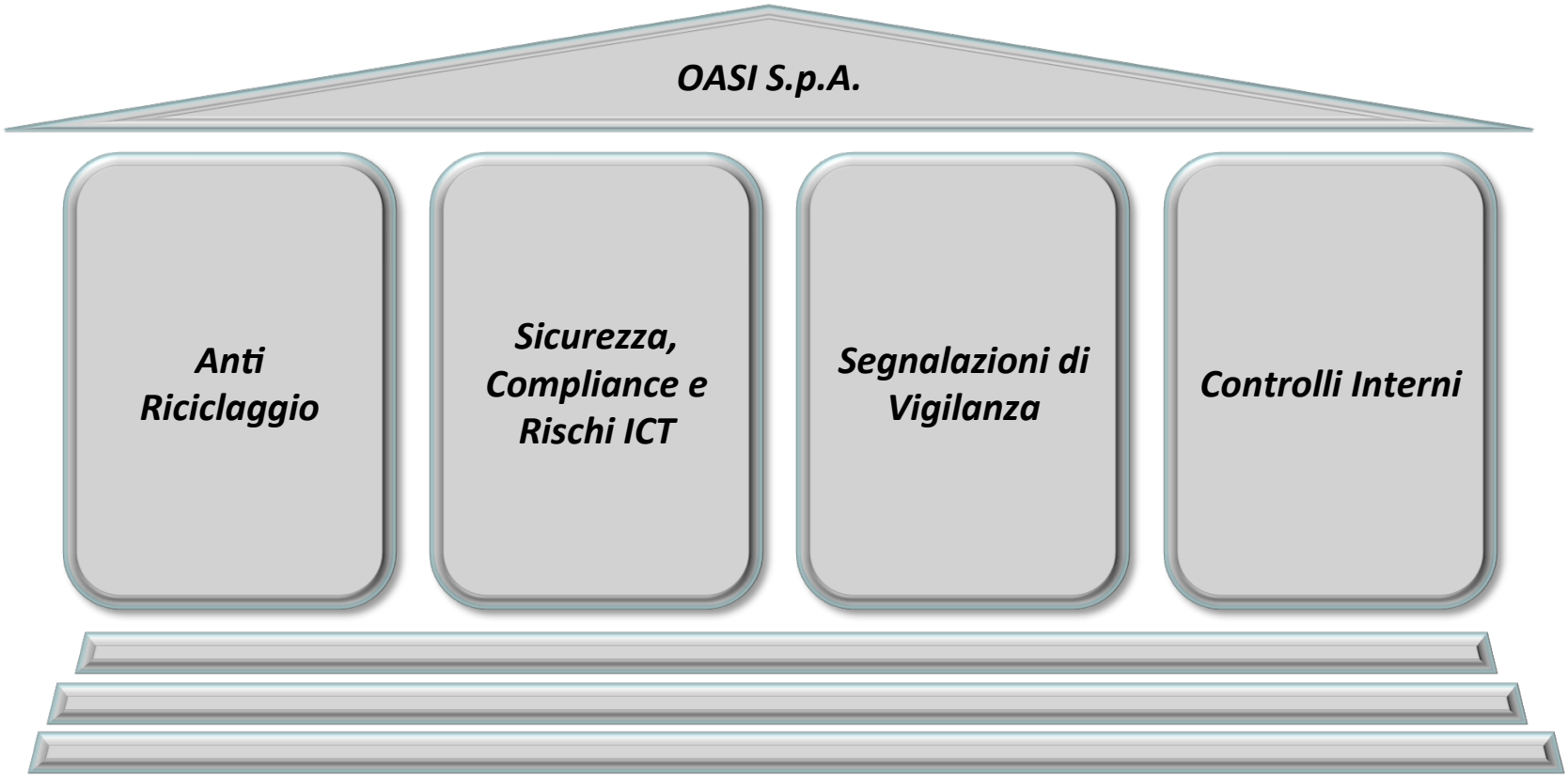
Privilegiare la **cooperazione** con **attori di sistema** e con altre banche / PSP per orientare al meglio i **significativi sforzi** e **investimenti** da conseguire per garantire la **conformità** con i requisiti di **sicurezza** espressi a livello europeo da **EC**, **BCE** e **EBA**

Agenda dell'intervento

- Premessa: il contesto di riferimento in tema di e-payments, cybersecurity ed e-identity
- Un modello di riferimento per la sicurezza di un sistema di e-payments
- Raccomandazioni per banche / PSP in tema di sicurezza dei servizi di e-payments
- ***Il posizionamento di Oasi S.p.A. e del Gruppo ICBPI in materia di sicurezza degli e-payments***

OASI è la società del Gruppo ICBPI specializzata nello sviluppo / integrazione di soluzioni informatiche e nei servizi di consulenza, outsourcing e formazione

OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A. è la società del gruppo ICBPI leader nelle soluzioni, nella consulenza, nei servizi innovativi e nell'outsourcing in tema di antiriciclaggio, controlli interni, sicurezza, rischi e compliance ICT e segnalazioni di vigilanza



Oasi S.p.A. ha predisposto un'offerta completa di servizi e soluzioni innovative in materia di sicurezza, compliance e rischi ICT

Ambito	Consulenza	Soluzioni	Servizi / outsourcing
Sicurezza Informatica	- Policy, procedure e processi - Gestione rischio informatico - IT auditing - Conformità Privacy - Certificazioni ISO 27001 - Revisione contrattualistica - Conformità Circ. 263/2006 - Sistemi di reportistica	- Gestione dei log di sicurezza - Classificazione delle informazioni - Data Loss Prevention - Protezione degli endpoint - Gestione del rischio informatico - Advanced Threat Prevention	- Monitoraggio della sicurezza IT - Computer forensics - Vulnerability / penetration test - Revisione del codice sorgente
Antifrode e-payments	- *Policy, procedure e processi* - *Gestione rischio frode* - *Verifiche di conformità* - *Conformità Racc. BCE*	- *Strong Authentication* - *Transaction monitoring*	- *Anti phishing / malware* - *Active Fraud Prevention* - *Firma Digitale* - *Monitoraggio canale CBI*
Continuità Operativa	- Analisi degli impatti - Piani di Continuità Operativa - Piani di Disaster Recovery - Verifiche conformità - Certificazioni ISO 22301 - Revisione contrattualistica - Conformità Circ. 263/2006	← - SW per la gestione del piano di BC - SW per la gestione delle crisi →	
Sicurezza Fisica	- Policy e procedure - Gestione rischio rapina - Contrattualistica - Sistemi di reportistica	- SW Gestione apprestamenti - SW Gestione dei mezzi forti - SW Gestione degli allarmi	- Formazione del personale - Assessment di filiali - Assessment sedi direzionali

Dettaglio offerta Oasi in tema di contrasto alle frodi sugli *e-payments* (1 / 2)

Ambito	Descrizione
Consulenza	–Supporto alla predisposizione della **Politica** per la **sicurezza dei servizi di pagamento** resi disponibili alla clientela sul canale **Internet / Mobile** , in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati via Internet / Mobile
	–Supporto alla predisposizione della **procedura** per la **gestione degli incidenti di sicurezza** sui **servizi** di **pagamento** resi disponibili alla clientela sul canale **Internet / Mobile**, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati via Internet / Mobile
	–Supporto alle attività di analisi, gestione e monitoraggio dei **rischi di frode** relativi ai servizi di **pagamento** via **Internet / Mobile** in relazione ai principali impatti (operativi, conformità, immagine) che ne possono derivare, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati via Internet / Mobile
	–Supporto alla conduzione di attività di **valutazione**, **gap analysis** e **remediation plan** in relazione allo stato della normativa, dei processi, delle soluzioni e dei controlli in tema di sicurezza dei servizi di pagamento resi disponibili alla clientela sul canale Internet, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati via Internet / mobile
	–Supporto alla predisposizione di **dashboard** con **metriche** di sintesi per la **reportistica** e i **flussi informativi** direzionali e operativi in tema di contrasto alle frodi sui canali Internet / Mobile
	–Supporto alle attività di **vendor selection** e disegno **modelli operativi** / **architetture informatiche** per soluzioni di contrasto alle frodi (e.g. strong authentication, transaction monitoring, adaptive authentication, …) sui canali Internet / Mobile

Dettaglio offerta Oasi in tema di contrasto alle frodi sugli *e-payments* (2 / 2)

Ambito	Descrizione
Soluzioni	–Fornitura e integrazione di soluzioni (e.g. token OTP, mobile OTP, transaction signing, …) per la **strong authentication** della clientela retail e corporate ai servizi remote banking via internet / mobile, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati su Internet
	–Fornitura e integrazione di soluzioni di **monitoraggio** delle **transazioni** per il monitoraggio dell'operatività effettuata con canali bancari remoti (Internet, telefono, mobile) ai fini dell'identificazione di transazioni ritenute fraudolente, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti su Internet
Servizi	–Erogazione di un **servizio** di **monitoraggio delle transazioni**, tramite un presidio specialistico di I / II° livello operante in modalità H24, sulle piattaforme di remote banking del cliente, finalizzato alla rilevazione di tentativi di frode, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati su Internet
	–Erogazione di un servizio per il **contrasto alle minacce** Internet (tramite le tecniche cosiddette di phishing e malware) di **furto delle credenziali** di accesso ai servizi di remote banking per la clientela retail e corporate, in linea con le Raccomandazioni BCE per la sicurezza dei pagamenti effettuati su Internet
	–Erogazione di servizi di **Firma Digitale a valenza legale** (ICBPI è iscritta all'Elenco Pubblico dei Certificatori accreditati dall'Agenzia per l'Italia Digitale) quali certificati e dispositivi per la firma digitale locale, servizio di firma digitale remota e massiva, firma elettronica avanzata, servizio di marcatura temporale e di conservazione sostitutiva

Grazie per l'attenzione

Ing. Andrea Agosti
Responsabile Servizio Security

OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A.
Azienda del Gruppo Bancario Istituto Centrale delle Banche Popolari Italiane
Corso Europa, 18 - 20122 Milano - Tel. +39 02 77051
Cell.:**+39 335 7365157** Ufficio: **02 7705326** Mail: **a.agosti@oasi-servizi.it**