Usare gli "*attributi*" per il contrasto alle frodi

Milano, 16 Maggio 2023

BANCHE E SICUREZZA

NTT DATA
Trusted Global Innovator

NTT DATA

INDICE

IL RISCHIO DELLE FRODI NEL SETTORE BANCARIO

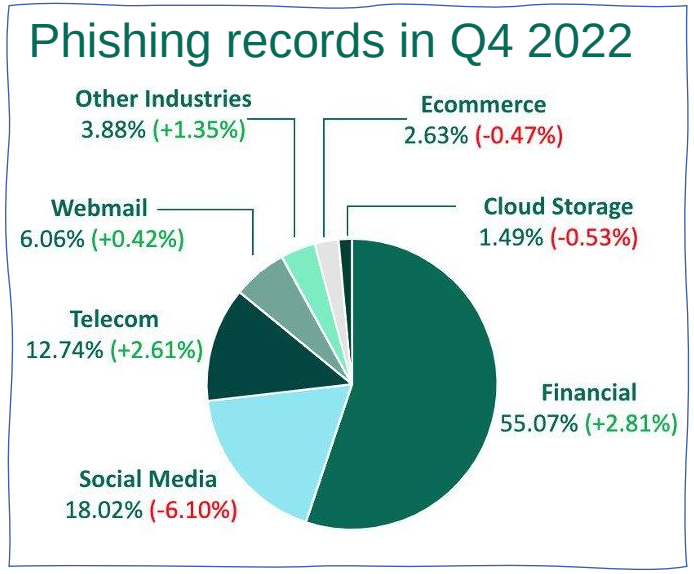
NTT DATA

Per ovvie ragioni, ***Banche ed Istituti Finanziari*** (o meglio, i loro Clienti) sono tra le ***vittime preferite dei frodatori***.
Nel 2022 il settore è stato principalmente preso di mira dal ***phishing*** per ***furto di credenziali*** attraverso siti web malevoli.

I siti di ***phishing*** che si spacciano per organizzazioni rispettabili continuano a rappresentare la ***principale minaccia online*** per le aziende e i loro marchi.

Nel IV trimestre del 2022, *più della metà di tutti i siti di phishing ha impersonato istituzioni finanziarie*, con attori che utilizzano marchi falsi per indurre le vittime a rivelare credenziali di accesso e altre informazioni sensibili.
Quello finanziario ha registrato il maggiore aumento tra tutti i settori, con una crescita di quasi il 3% in quota rispetto al terzo trimestre.

All'interno del gruppo, le *banche a diffusione nazionale* (*storicamente il principale obiettivo impersonato tra gli istituti finanziari*) sono cresciute di oltre il 15% della quota, rappresentando il 71,30% del totale dei siti di phishing.



[Fonte: FORTRA PhishLabs]

CONTROMISURE

In considerazione del rischio di frodi nel settore bancario, come prescritto anche dalla normative PSD-2, è necessario sfruttare ***opportune soluzioni tecnologiche*** per contrastare questo fenomeno.

Strong Customer Authentication (SCA)

Assicurarsi dell'***identità del Cliente***, basandosi su ***più fattori di autenticazione di tipo diverso***. (Evitare che un fattore di autenticazione possa essere *ingenuamente comunicato* da un legittimo cliente ad un frodatore…)

Dynamic Linking

Assicurare un ***«collegamento dinamico»*** tra l'***operazione bancaria***, l'***importo*** ed il ***beneficiario*** specificati al momento di disporre l'operazione. Il collegamento dinamico è possibile attraverso *OTP* o altre conferme basate sulla *crittografia*.

Risk-Based Authorization (RBA)

Utilizzare tecniche evolute (*behavioral analysis*) per identificare in tempo reale ***transazioni sospette*** (per il profilo di un certo cliente) in modo da bloccarle preventivamente, o richiedere un livello ulteriore di controllo.

A causa di tecniche malevole di *social engineering*, il *fattore umano* è l'*anello debole*. La *tecnologia* dovrebbe essere usata per proteggere dai frodatori anche gli *utenti "ingenui"*.

Attribute Based Encryption (ABE)

ECCELLENZA NEL MONDO DELLA CRITTOGRAFIA

NTT DATA

I laboratori di R&D del Gruppo NTT costituiscono un ***Centro di Eccellenza sulla Crittografia***, riconosciuto a livello mondiale.

Front-line Researchers

Aiming to Be the World's Top Cryptography Laboratory

Tatsuaki Okamoto
NTT Fellow, Director, Cryptography & Information Security Laboratories, NTT Research, Inc.

Overview

Information and communication technology is used in all types of business activities, and expectations concerning security and reliability of cryptography—which is key to information security measures—are increasing. We asked Dr. Tatsuaki Okamoto, an NTT Fellow who spearheads the Cryptography and Information Security Laboratories (CIS Labs) of NTT Research, Inc., employing top scientists in cryptography and blockchains, about the progress of CIS Labs and his attitude toward being a distinguished researcher.

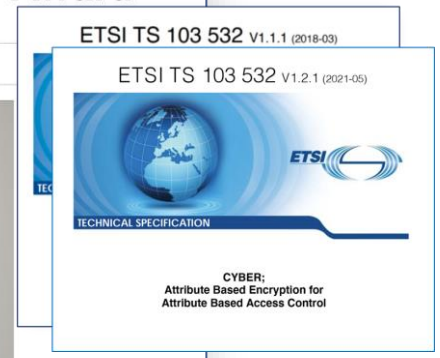
Keywords: cryptography, blockchain, attribute-based encryption

NTT Research Distinguished Scientist Brent Waters & UCLA Professor Amit Sahai Win IACR Test-of-Time Award

NTT Research Staff April 9, 2020

Paper Co-Authored in 2005 Introduced Groundbreaking Concept of Attribute-Based Encryption

NTT Research, Inc., a division of NTT (TYO:9432), today announced that a paper co-authored in 2005 by Dr. Brent Waters, a distinguished scientist in its Cryptography and Information Security (CIS) Lab, has won an International Association for Cryptologic Research (IACR) Test-of-Time Award. Dr. Waters and Dr. Amit Sahai, a professor of computer science at the UCLA Samueli School of Engineering, delivered their paper, "Fuzzy Identity-Based Encryption," at the 2005 Eurocrypt conference. The paper introduced attribute-based encryption, in which policy rather than individuals determines who can encrypt.



ATTRIBUTE BASED ENCRYPTION (ABE)

NTT DATA

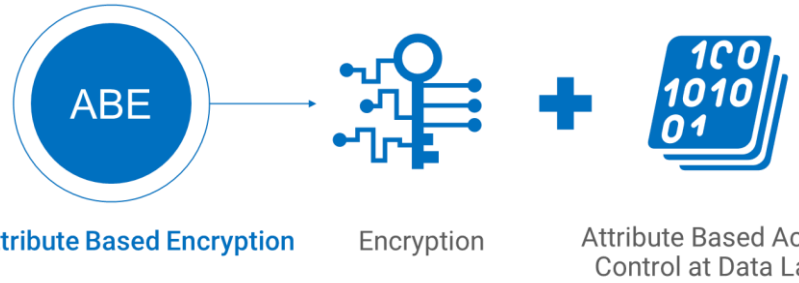
NTT Research ha proposto la teoria alla base di ABE e i nostri laboratori di R&D guidano gli sviluppi di questa tecnologia.
NTT DATA Italia ha collaborato direttamente all'implementazione di un layer di API per le funzioni crittografiche.

ABE è un innovativo paradigma di ***crittografia asimmetrica*** che consente di definire in maniera molto granulare le *autorizzazioni di accesso ai dati*, incorporandone il controllo direttamente nelle funzioni crittografiche.

Il meccanismo si basa sui seguenti elementi:

- Un ***chiave di cifratura*** ed una corrispondente ***famiglia di chiavi di decifratura*** associate
- Una serie di ***attributi*** (valori numerici, booleani o stringhe)
- Una ***policy*** (espressione booleana costruita sulla base degli attributi)

Un dato cifrato usando ABE può essere decifrato da una chiave di decifratura se e solo se gli attributi forgiati nella chiave [o nel cyphertext] soddisfano la policy forgiata nel cyphertext [o nella chiave].

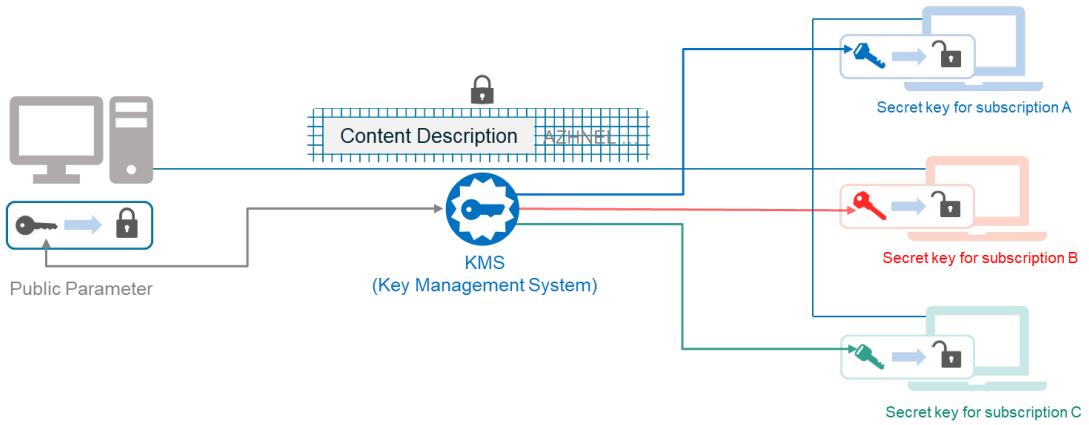


- I dati possono essere ***cifrati con una singola chiave***, e ***decifrati*** selettivamente ***dalle chiavi di decifratura che soddisfano la policy*** stabilita in fase di cifratura
- L'***autorizzazione all'accesso ai dati*** non è delegata (solo) alla logica applicativa (application layer), ma è nativamente ***incorporata nelle operazioni crittografiche*** (data layer)
- La ***capacità di decifrare un cyphertext*** dimostra il ***soddisfacimento di una policy*** definita su specifici attributi, ***senza dover fare disclosure degli attributi***

DUE DECLINAZIONI: KP-ABE E CP-ABE

***KP-ABE**: La policy è forgiata nella chiave di decifra e gli attributi sono forgiati nel cyphertext*
***CP-ABE**: Gli attributi sono forgiati nella chiave di decifra e la policy è forgiata nel cyphertext*

KP-ABE

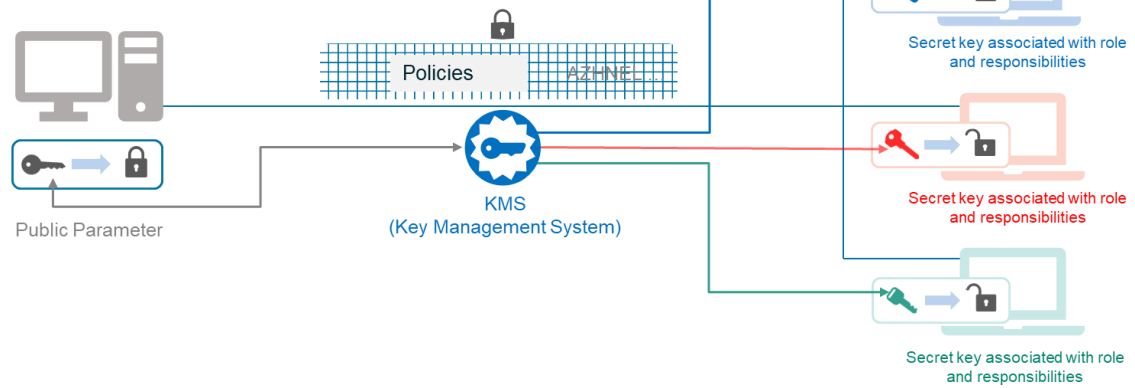


Content Distribution / Content based Access Control

- La content description è specificata attraverso attributi del cyphertext
- La secret key incorpora una policy che esprime i privilegi dell'utente
- Autorizzazione: i privilegi dell'utente specificati nella policy della sua secret key sono tali da decifrare un contenuto (caratterizzato da certi attributi)
- Access policy change: cambiare la secret key dell'utente

ESEMPIO: sottoscrizione a contenuti in pay-per-view

CP-ABE



Secure Data Sharing / Role based Policy

- L'access policy è embedded nel dato/file cifrato
- La secret key identifica ruolo e responsabilità del destinatario
- Autorizzazione: gli attributi della secret key (che rappresentano ruoli e responsabilità) soddisfano una policy predefinita (associata al dato)
- Access policy change: effettuare re-encrypt dei dati specificando la nuova policy

ESEMPIO: Dati accessibili a seconda del ruolo aziendale; attributi del ruolo aziendale associati alla chiave assegnata ad un dipendente

ABE SARÀ PRESTO QUANTUM RESISTANT

NTT DATA

Il Gruppo NTT è molto attivo nella ricerca sulla ***Post Quantum Cryptography***, ed alcuni tra i migliori crittografi del mondo stanno lavorando per rendere ABE inviolabile anche da futuri attacchi realizzati con Quantum Computers.

NTT Research

NTT Research ha già realizzato una PoC e ***presto*** verrà rilasciata una versione di Attribute Based Encryption che sarà ***Quantum Resistant***.

Creating Post-Quantum Cryptography for Attribute-Based Encryption

December 1, 2022

Introduced in a 2005 paper co-authored by NTT Research Cryptography & Information Security (CIS) Lab Director Brent Waters, attribute-based encryption (ABE) is now approaching commercialization. As a case in point, NTT is conducting a proof-of-concept (POC) information-sharing platform using ABE with the University of Technology Sydney (UTS). Part of a broader technology partnership with UTS, this initial platform is aimed at internal UTS applications. As more evidence for the growing maturity of this encryption scheme, NTT Research recently conducted an ABE hackathon that drew five NTT global teams to Sunnyvale, where they spent two weeks building potential implementations of the technology.

Compared to the prevailing coarse-grained access model of public-key encryption, where giving out a secret key essentially amounts to giving access to all the encrypted data, ABE is a more finely tuned approach that grants prescribed access of encrypted data to someone with a set of matching traits. The checking of those attributes happens mathematically, "inside the crypto," which shifts attention away from servers or software engineering and toward policies and the encryption itself. In addition to exploring the commercialization of ABE through its Technology Promotion Team, which organized the recent hackathon, NTT Research is also engaged in basic research into post-quantum ABE schemes.

One relatively recent paper on the subject was co-authored by Dr. Waters and CIS Lab Scientists Pratish Datta and Ilan Komargodski. Titled "Decentralized Multi-Authority ABE for DNFs from LWE," and presented at EuroCrypt 2021, the Datta, Komargodski and Waters (DKW) paper presents the first collusion-resistant, post-quantum decentralized multi-authority (MA)-ABE scheme. It is proved under the Learning with Errors (LWE) assumption, which has become a pillar in post-quantum security. The scheme also supports access policies captured by disjunctive normal form (DNF) formulas, which are useful in automated theorem proving.

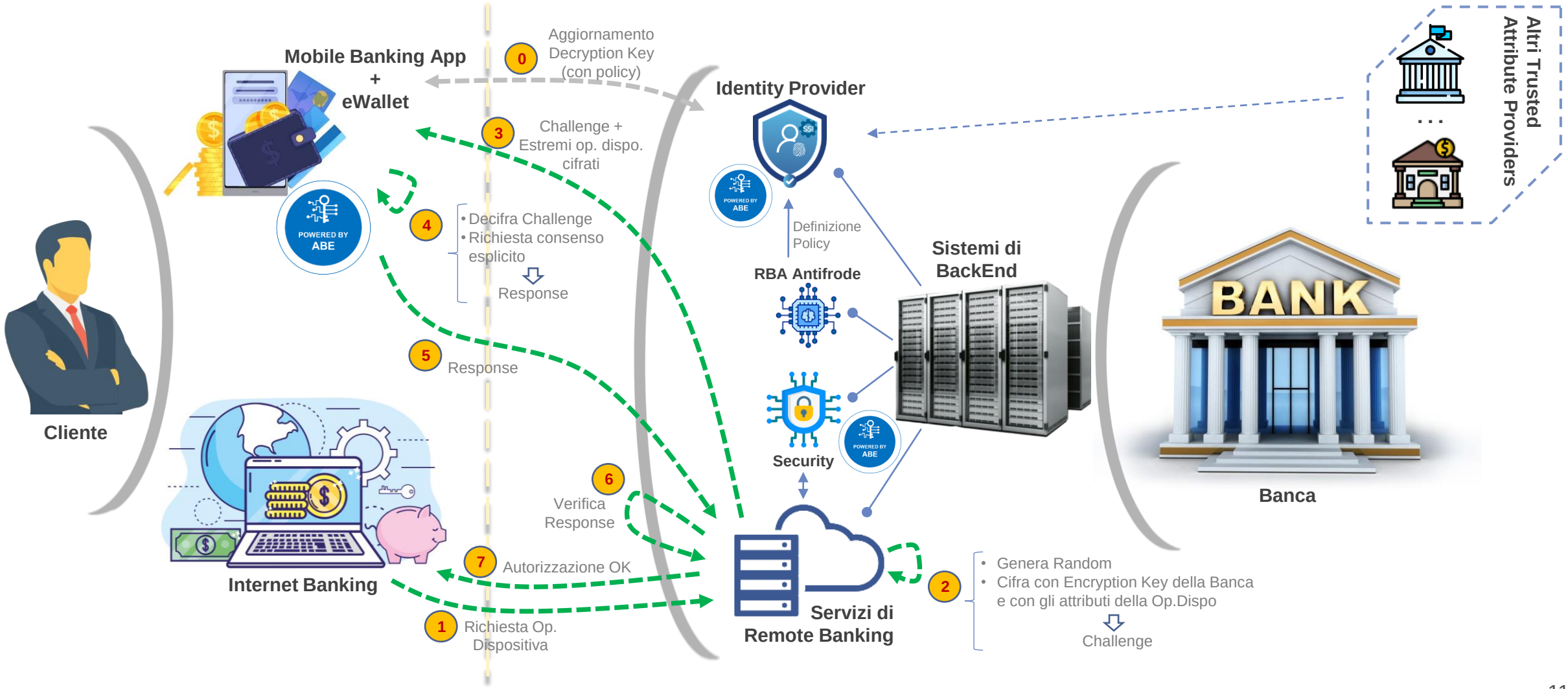
"The rapid advances in internet communications, social networking platforms, electronic payments, and cloud technology have already created the need for highly sophisticated security infrastructures for which the basic public-key encryption no longer suffices," Dr. Datta said in an interview. "ABE has emerged as a promising tool for deployment in such advanced security infrastructures. This has motivated us to develop post-quantum secure ABE schemes to protect these advanced security infrastructures against quantum adversaries, so that the advent of quantum computers cannot disrupt the digital services built on top of those security infrastructures." (For more on Dr. Datta and additional comments on the EuroCrypt 2021 paper, see this recent profile and Q&A.)

So far, the NTT Research Technology Promotion Team has implemented a prototype of the scheme, but not yet the full MA-ABE. The team, led by Takashi Goto, is conducting tests for decryption correctness and performance. To be deployed commercially, however, Mr. Goto said it would need to undergo further adaptation. "Although practical quantum attacks do not constitute an imminent threat," Mr. Goto said. "NTT customers can rest assured that some of the world's top cryptographers are exploring post-quantum ABE solutions, and that NTT will provide migration paths down the road."

Uso di ABE per il contrasto alle frodi bancarie

AUTORIZZAZIONE DELLE OPERAZIONI DISPOSITIVE

E' possibile usare ABE (*formulazione KP*) per implementare un meccanismo di ***Autorizzazione delle Operazioni Dispositive bancarie***; inoltre ABE (*formulazione CP*) può essere usato per implementare un ***privacy-preserving eWallet***.



POTENZIALI BENEFICI DI QUESTO APPROCCIO

Secondo l'approccio proposto, le abitudini di spesa del cliente (***modello comportamentale***) verrebbero tradotte in un ***formalismo di policy*** molto ***flessibile e granulare***. L'adozione di un ***meccanismo di autorizzazione basato su ABE*** avrebbe diversi ***benefici***…

Sicurezza

Unificare le funzionalità di ***autenticazione, autorizzazione e trasmissione cifrata dei dati***, ed implementarle al ***layer crittografico*** (piuttosto che a quello applicativo) rende il ***processo complessivamente più sicuro***.

Riduzione del rischio di frodi

L'utilizzo della KP-ABE rende più ***difficile per gli attaccanti compromettere il sistema di autorizzazione ed il processo E2E***; ciò può aiutare a ***ridurre il rischio di frode*** e garantire una maggiore sicurezza per le transazioni bancarie.

Policy granulari e flessibili

KP-ABE consente di creare ***policy di autorizzazione molto precise***, basate su un ***set estensibile di attributi***, ***personalizzate per ciascun cliente***, ***dinamiche***; questo approccio consente *più accuratezza e flessibilità rispetto ai sistemi RBA tradizionali*.

Auditability e non ripudio

Esaminando le policy associate alle chiavi KP-ABE distribuite, si possono ***ricostruire a posteriori le logiche che hanno portato ad autorizzare determinate transazioni***; grazie al challenge/response si ha una ***prova crittografica inequivocabile*** che l'utente ha autorizzato la transazione.

Scalabilità e decentralizzazione dell'autorizzazione

Il ***processo di autorizzazione*** (basato sulla capacità dell'utente di decifrare il challenge) è ***decentralizzato*** e non dipende interamente dal BE della Banca (riducendone il carico di lavoro); ABE è molto ***scalabile nella gestione delle chiavi*** ed è adatto per l'uso in grandi istituti con *molti clienti e transazioni*.

Riservatezza e protezione della privacy

Le logiche di autorizzazione sono riservate, non esposte come nelle tradizionali RBAC (Rule-Based Access Control). Poichè il meccanismo è intrinsecamente basato sulla crittografia, ***gli attributi e i dati sono protetti***, preservando la ***privacy degli utenti*** e le loro transazioni.

ALTRE POSSIBILI APPLICAZIONI DI ABE NELLE BANCHE

Attribute Based Encryption è una tecnologia crittografica che può abilitare ***diversi use cases***.

Privacy-preserving eWallet

La tecnologia CP-ABE potrebbe essere usata per creare un «trusted ecosystem» in cui un eWallet raccoglie una serie di attributi che caratterizzano un utente.

Subscription a servizi a pagamento

La tecnologia KP-ABE potrebbe essere usata per implementare il controllo accessi a servizi, in cui l'abbonamento sottoscritto è rappresentato dalla decryption key.

Content distribution

La tecnologia KP-ABE potrebbe essere usata per distribuire documenti strutturati, porzioni dei quali sono decifrabili dagli utenti in modo selettivo in base al contenuto.

Secure data sharing

La tecnologia CP-ABE potrebbe essere usata per creare un repository di documenti cifrati, accessibili agli utenti in base al loro ruolo (definito attraverso attributi).


NTT DATA
Trusted Global Innovator
Grazie!