Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on Advancing Privacy Enhancing Technologies

NTT Research

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

NTT Research, Inc.
940 Stewart Dr, Sunnyvale, CA 94085, USA
URL: http://www.ntt-research.com

July 8, 2022

Ms. Stacy Murphy
Operations Manager
White House OSTP

Dear Ms. Stacy Murphy:

I appreciate the opportunity to respond to OSPT's RFI on Advanced PET.

NTT Research is NTT R&D's global presence outside of Japan with headquarter based in Bay Area of US. We expand a rich lineage of ground-breaking basic research heritage from Japan to the rest of the world. One of our key research topics in cryptography and information security area is Attribute Based Encryption (ABE) / Functional Encryption (FE). We would like to highlight the unique roles ABE/FE can play in many of the use cases for enhancing data privacy and security. We believe ABE/FE's characteristics are complementary to other PETs. Lastly, we also would like to provide you with our observations and feedback about the challenges and barriers in adopting PET.

If there is anything we can clarify for you further, please feel free to reach out directly to me or my staff member, Fang Wu

Sincerely,

Kazuhiro Gomi
President and CEO
NTT Research, Inc.

This page intentionally left blank

NTT Research, Inc.
940 Stewart Dr, Sunnyvale, CA 94085, USA
www.ntt-research.com

RESPONSE TO OSTP RFI ON ADVANCING PRICACY-ENHANCING TECHNOLOGIES

July 8, 2022

Table of Contents

Table of Figures

Executive Summary

NTT Research is NTT R&D's global presence outside of Japan with headquarter based in Bay Area of US. As an organization that has some elements of a public utility and some elements of a private company, NTT Group makes full use of various business resources and capabilities, including research and development, ICT infrastructure and personnel, to solve social issues by promoting digital transformation and CSR through collaborations with our partners. NTT Research expands a rich lineage of ground-breaking basic research heritage from Japan to the rest of the world. Our current focus research areas are:

- physics and informatics
- medical and health informatics
- cryptography and information security

One of our key research topics in cryptography and information security is Attribute Based Encryption (ABE)/Functional Encryption (FE). While ABE and FE have been recognized as part of the Privacy Enhancing Technologies, e.g., by NIST Privacy-Enhancing Cryptography (PEC) project, they have been overshadowed by technologies such as FHE (Full Homomorphic Encryption). We would like to highlight the unique roles ABE/FE can play in many of use cases for enhancing data privacy and security. We believe ABE/FE's characteristics are complementary to other PETs. Lastly, we also would like to provide our observations and feedback about the challenges and barriers in adopting PET. In fact, a number of these factors contribute to slow adoption of ABE even though the technology is mature and can provide benefits to enhance data privacy and data security.

1 Introduction

1.1 Attribute Based Encryption (ABE)

Legacy encryption technologies have been an "all-or-nothing" proposition. For any given encrypted dataset, or ciphertext, if you had the correct key to open it, you had access to the entire dataset. If you didn't have the appropriate key, you could access none of it.

In 2005, cryptographic researchers Brent Waters and Amit Sahai changed that dynamic with a paper that introduced the concepts of attribute-based encryption. The paper[i], titled "Fuzzy Identity-based Encryption," introduced the idea that multiple keys could exist for a given ciphertext to enable different users to access different parts of the underlying dataset with attribute-based access control policy. This idea opens up new use cases and applications for cryptography in information security and data protection. Over the years, a lot of more research has been done. ABE algorithms have been proven to be secure and enhanced to be increasingly efficient. With current state of the computing technologies, ABE is ready to be deployed in production environment for many practical use cases.

Moreover, ABE can be upgrade to a quantum-resistant algorithm by swapping the underline cryptographic library to a post quantum cryptography algorithm. Moreover, this upgrade can be transparent to applications. The NTT implementation demonstrates such transparency for easy migration to post quantum cryptography.

ABE provides the ability to implement Attribute-Based Access Control (ABAC) at cryptographic layer. ABAC is a powerful way to enforce data access policy for data privacy and data security. The concept has been around for a long time. NIS published a guideline in this area[ii]. With ABE, ABAC can be implemented in the way that is system independent because policy is embedded into encryption. Data sets can be encrypted with ABE to allow different data segments to have different ABAC access policies. Policy implemented with ABE supports “fine-grained” access control.

For example, only users tagged with an attribute of “financial team” can see financial related segment of the data set, and only users tagged with an attribute of “account support” can see customer contact information. Segment(s) of data sets in database implementation can be row(s), column(s), or even down to cell(s).

Embedding access control policy into encryption provides several benefits for data privacy and data security that will be demonstrated in our use case discussions later in this response.

1.2 Functional Encryption (FE)

Functional Encryption (FE) is a generalization of Attribute-Based Encryption (ABE)[iii]. It allows a user who has a proper key:

- to compute a specific function on encrypted data, and
- to obtain the computing result (unencrypted)

while the original data remains encrypted/protected.

Use cases involving delegating certain actions based on outcome(s) of computing result(s) on encrypted data are perfect for FE. A data owner can provide specific key(s) to third party to allow this third party to compute certain function(s) without decrypting original data. Based on the result(s) of computing function(s), the third party can take proper action(s) without the need to get the data owner involved in the process.

Unlike ABE (even though ABE can be viewed as a specialization of FE), full functionality of FE is not yet ready for production. More research in this area is needed to realize its full potential.

2 ABE Use Cases

Until recently, most of the use cases identified for ABE are related to data protection. Digital Identity and Verifiable Credential (VC) emerge as new applications. ABE provides flexibility to support a wide range digital credential verification use cases from “full knowledge proof” to “Zero Knowledge Proof”.

2.1 Data Security and Data Privacy

As organizations increasingly deploy AI/ML capabilities and adopt data driven decision making processes, data becomes one of the most valuable assets. On the other hand, data related to personal privacy needs to be properly handled and protected. Moreover, today's hostile cybersecurity environment demands organizations to eliminate every single potential vulnerability for data breach. All these factors ask for better data protection for privacy and security. There are several limitations with legacy ways of protecting data. ABE can be used to bridge these gaps.

ABE provides data privacy enhancements and protection to sensitive data in database, data lake, lake house, data warehouse, blockchain or entire data asset of an organization. The key benefit is the ability to embed access control policy into encryption, so that consistent access control can be enforced starting from the point the data is created throughout the entire life cycle regardless of where it gets moved or stored. The end results are:

- empower data owners to have full control of their data through entire life cycle with consistent access control policy
- allow organizations to have better data governance
- reduce policy configuration overhead
- minimize large scale data breach

2.1.1 Challenges of legacy systems

2.1.1.1 System Based Access Policy Limitations

Many organizations deploy multiple systems for data storage/process (see " Figure 1: legacy way of access control policy configurations"). Data is created at the data source and flows through multiple systems to downstream, e.g., data lake for analytics/ML/AL purpose. Implementing access control policy in a consistent way for every system is a challenge task. Often time, configurations for all systems are required to achieve such goal. Multi-system configurations come with overhead that consumes resources and drives up cost.

Moreover, system-based access control policy can only be applied and enforced to data residing inside of given system(s). Once the data is sent out, downloaded, leaked, or hacked out of protection boundary, there is no access control policy enforcement anymore.

Lastly, because system-based access control needs system specific knowledge to make necessary configuration(s), most of data owners do not have the ability to perform such task(s) unless another layer of system being deployed for policy building. These configurations most likely rely on members of system admin personnel. As a result, system admin personnel might have access to sensitive data that they are not supposed to access to if proper processes and/or system capabilities are not in place - data privacy and data security might be compromised.

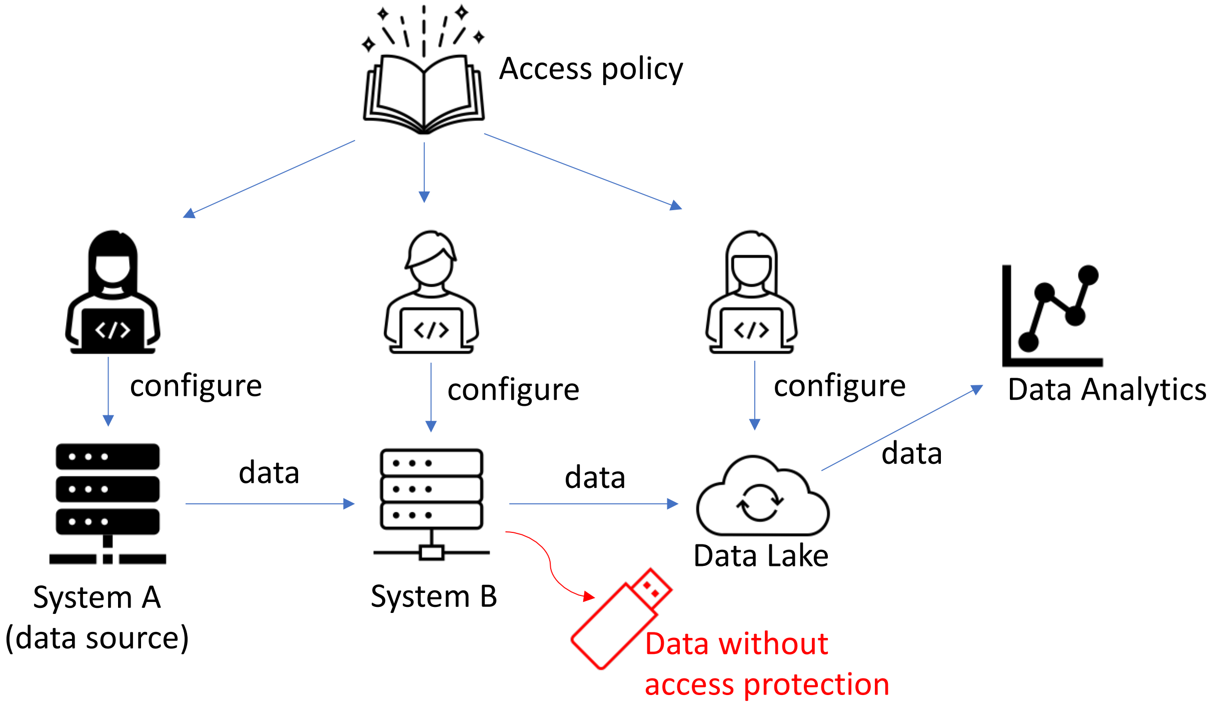
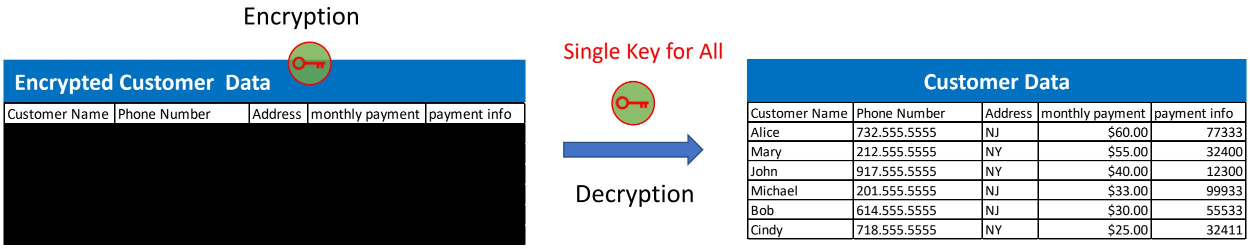


Figure 1: legacy way of access control policy configurations

2.1.1.2 Legacy Data Encryption Limitations

To protect sensitive data, legacy encryption is often utilized. However, while legacy encryption technologies such as AES provide high degree of security for data protection, there is a single decryption key being used by all users in daily operation. Once the decryption key is hacked with the encrypted data, all data will be exposed (see Figure 2 legacy data encryption - "all or nothing"). "All or nothing" access is too vulnerable for large scale data set such as customer database.



Customer Name	Phone Number	Address	monthly payment	payment info
Alice	732.555.5555	NJ	$60.00	77333
Mary	212.555.5555	NY	$55.00	32400
John	917.555.5555	NY	$40.00	12300
Michael	201.555.5555	NJ	$33.00	99933
Bob	614.555.5555	NJ	$30.00	55533
Cindy	718.555.5555	NY	$25.00	32411

Figure 2 legacy data encryption - "all or nothing"

2.1.2 ABE to Address the Issues

ABE encryption can be applied when data is created or as close to the point that the data is created (see " Figure 3 ABE access control policy for entire data lifecycle"). This provides several benefits in terms of data protection and large-scale data breach avoiding.

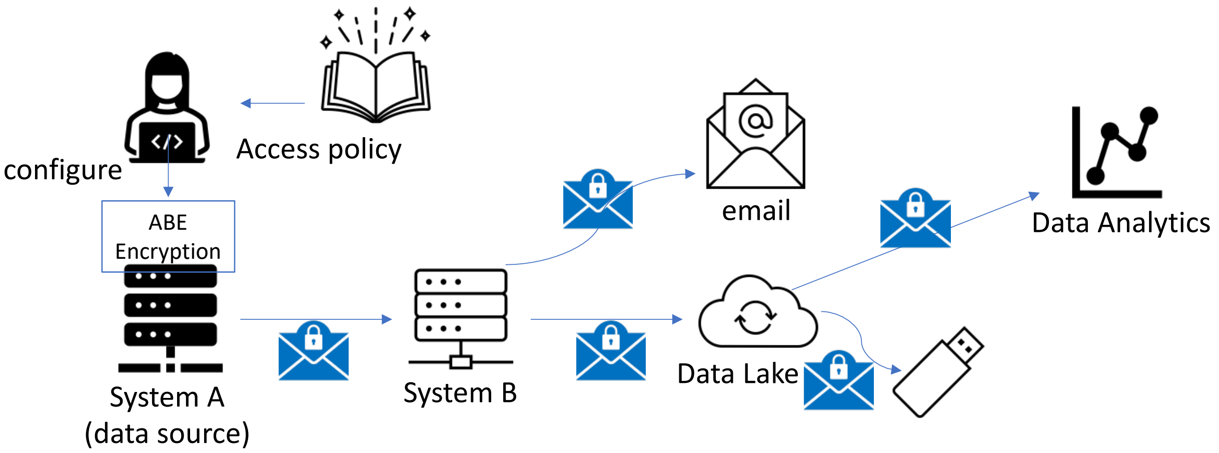


Figure 3 ABE access control policy for entire data lifecycle

2.1.2.1 Data Layer Access Control

Because data access policy of ABE is embedded in the data layer, this eliminates the need to configure system level access control policy on a system-by-system basis. With that, cost saving and resource efficiency can be achieved. It also provides the benefit of consistent policy flowing down with data from upstream to downstream, even for off-stream, e.g., download. Lastly, with proper policy builder deployed in conjunction with ABE, data owners can configure their own access control policy from upstream without worrying about any element of the policy being tempered or compromised when data flows down from one system to others.

2.1.2.2 Large Scale Data Breach Avoiding

2.1.2.2.1 Needed Basis Decryption Keys Instead of “Single Key for All”

ABE provides the ability to generate different user secret keys for different users with data access policy on a needed basis (see “ Figure 4 ABE Encryption: large scale data breach avoiding”). Only data segment(s) users have right to access can be decrypted instead of “single key for all”. Users use their own keys instead of a single decryption key used by all users in daily operation. As such, as long as there is proper protection for Key Generation System (KGS), possibility of large-scale data breach is decreased.

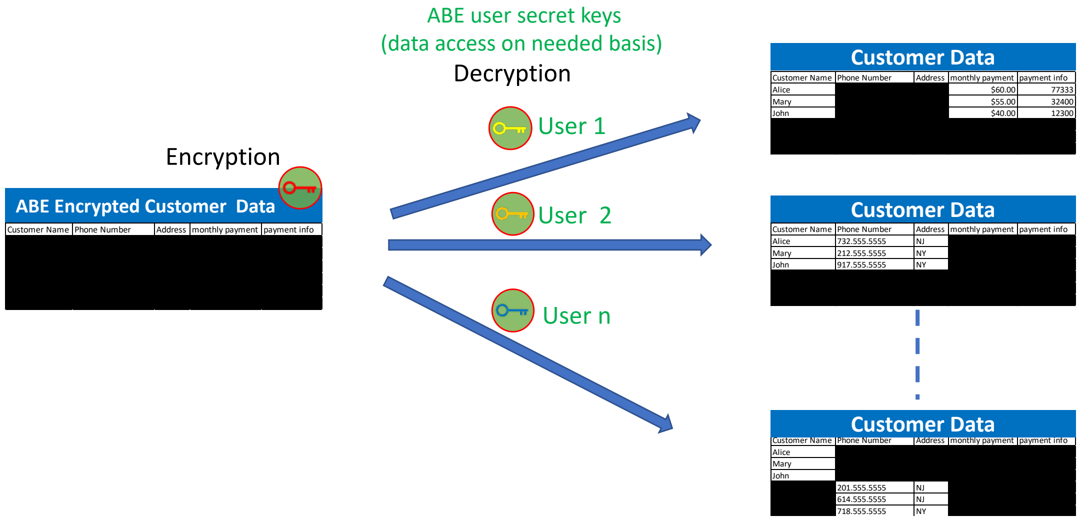


Figure 4 ABE Encryption: large scale data breach avoiding

2.1.2.2.2 Additional Layer of Security – Environmental Conditions

Additional security measures can also be implemented through environment/conditional attributes supported by ABE to ensure decryption keys only function in certain conditions, e.g., time of the date, specific location(s), network(s), device(s), and such. Proper access policy with these conditional attributes makes it harder for hackers.

2.2 Digital Identity and Verifiable Credential

Recent research expands ABE use cases from data protection to Digital Identity and Verifiable Credential (VC). [iv]

2.2.1 Different Use Cases of Digital Identity and Verifiable Credential

Different use cases might have different requirements for identity/credential verifications. Individuals to be verified can be completely anonymous for some use cases. For other use cases, they are required to provide a set of detailed identity attribute(s), and these attribute(s) need to be verified. There are also use cases falling in between:

- Individuals need to be verified of detailed information of identity and personal information ("full knowledge proof"):
    - Banking, e.g., to open an account
    - Government agencies, e.g., airport security check
- Individuals can be completely anonymous ("zero knowledge proof"):
    - senior discount, youth discount, Low-income discount
    - Resident based discount: transportation, theme park ticket/admission, etc.
- Individuals need to be identified, but other detailed identity attribute(s) might not be required; only threshold verification for certain attribute(s) is required ("partial knowledge proof"):
    - Age restricted purchasing: alcohol, tabaco, recreation drug, lottery tickets, etc.
    - Age restricted admission: casino, gym, etc.
    - Income threshold qualification for rental applications

ABE can be used to support all these use cases with added value in comparing to the current ways of operations as well as other potential technologies.

2.2.2 ABE for Digital Identity and Verifiable Credential

A high-level architecture is depicted in " Figure 5 ABE for verifiable credential concept":

- Identity Authority or Trusted Service Providers: This is an entity to maintain/to collect and to proof identity data; it also performs user authentication and ABE key generation.
- Person: S/he registers with Identity Authority to allow her/him to obtain digital identity in the form of ABE user key
- ABE user key represents digital identity containing identity attributes such as ID #, name, etc.
- Identity Verifiers: These are business or agencies that need to verify individual's identity for different use cases such as age restricted purchase, banking activities and such.
- Verification Steps:
  1. Person gets authenticated from Identity Authority and obtains digital ID, i.e., ABE user key containing person's identity attributes, e.g., passport #, name, citizenship, DoB (Day of Birth), etc.
  2. Identity Verifier use ABE (public parameter of ABE) to encrypt a "secret value" as "challenge" to send to Person. The access policy of this ABE encryption corresponds to verification requirements of the use case, e.g.,
     - age threshold for supermarket senior discount
     - specific person's name, passport # and such for international flight boarding process
  3. If the person can use her or his ABE user key to decrypt and return the "secret value", verification is complete with a positive result. If not, the verification fails.

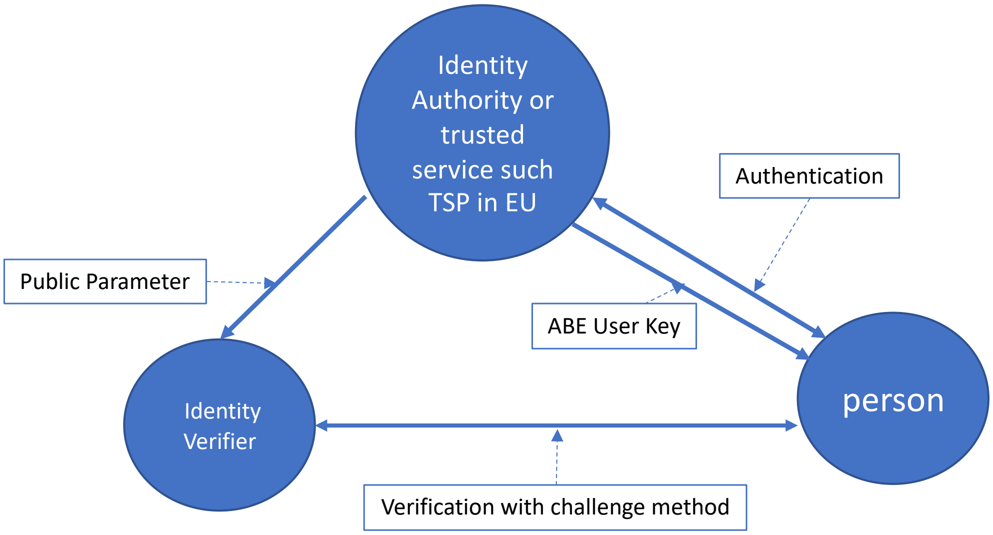

Identity Authority or trusted service such TSP in EU
Authentication
Public Parameter
ABE User Key
Identity Verifier
person
Verification with challenge method

Figure 5 ABE for verifiable credential concept

ABE provides the ability to use biometric attribute(s) to tie digital identity to individuals in a secure way for critical use cases:

- Biometric attributes can be range from a simple hash value of an individual's of ID photo to attribute(s) for more advanced technologies, e.g., three-dimensional facial recognition and iris recognition. The implementation can evolve along with technology innovation. This provides additional layer of security for preventing stolen keys being used for critical use cases.

Please see "Figure 6 biometric attribute(s) to add additional security" for illustration purpose:

- Person's user secret key contains hash value of ID photo as one of the identity attributes. Person provides the ID photo to airport along with other required identity info electronically.
- Airport uses the ID photo to inspect if it matches Person either by human inspection or facial recognition.
- If there is a match, Airport calculates hash value of the ID photo and uses it along with other needed identity attributes to form access policy for "challenge" for Person.
- If Person's ABE user key contains all proper attributes, e.g., ID photo hash value as well as other required attributes such as passport #, etc., Person can decrypt the "secret value" and return it to the airport inspection agent to complete the verification process.

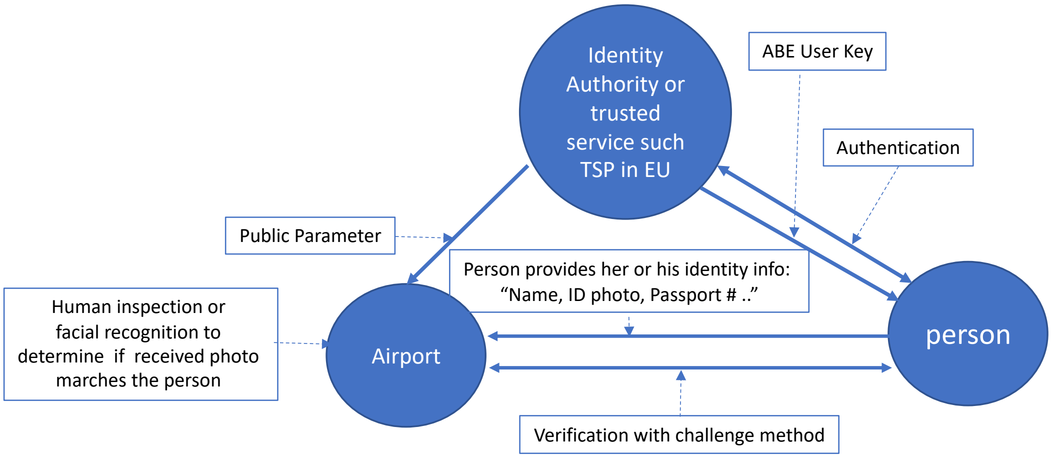

Identity Authority or trusted service such TSP in EU
ABE User Key
Authentication
Public Parameter
Person provides her or his identity info: "Name, ID photo, Passport # .."
Human inspection or facial recognition to determine if received photo marches the person
Airport
person
Verification with challenge method

Figure 6 biometric attribute(s) to add additional security

2.2.3 ABE Value Proposition for Digital Identity

ABE identity verification provides value for all use cases:

- "Full knowledge proof": Detailed credential verification:
  - All required attributes from an individual are verifiable through crypto technology with extremely low tampering possibility.
- "Zero knowledge proof": no detailed identity information is shared with verifiers while a given requirement can be verified, e.g., age threshold:
  - For the persons being verified: no worry about their identity information being stolen – everything is secured without privacy exposure.

  - For the verifiers (typically business entities): no need to touch PPI (Personal Private Information) data, it eliminates any liability as well as system requirements for handling PPI data.
- In comparing to the traditional physical ID, it eliminates the possibility of fake IDs being used as well as potential identity theft
- In comparing to software/system-based implementations, ABE provides much more secure and flexible ways in an end-to-end cryptographical fashion:
  - Attributes of user secret keys are generated by authorities or trust services, and they cannot be tampered for entire key cycle – from generation, to utilization, to expiration.
- Distributive verifications with only key generation relying on centralized system(s) – highly reliable architecture
- ABE provides multiple layers of added security protection:
  - the ability to tie digital ID to specific person by using biometric attribute(s)
  - the ability to tie digital ID to specific hardware/device with other environmental attributes
- Crypto technology of ABE provides a future proof evolution path in many ways, e.g., biometric attribute(s) can evolve along with technology innovation

3 Applications and Use Cases for Functional Encryption (FE)

Functional Encryption (FE) can be used for applications where it's useful to reveal just specific result(s) of the computing while original data remains to be encrypted/protected.

3.1 Secure Email Filtering

With FE encrypted email, several actions a user can delegate to email server to do without getting email content decrypted:

- To determine email message is spam, but without revealing the contents of the message
- Similarly, it could be used to determine whether an encrypted email is from important person(s), and thus flagged as "important," but again without revealing the contents

3.2 Surveillance

FE could be used to provide privacy preservation to individuals while a specific key to allow law enforcement to examine a series of surveillance photos to determine whether a particular person is included in an image – without revealing other contents of the images.

3.3 VPN Content Inspection

The Google Transparency Report[v] shows the percentage of encrypted web traffic has increased from less than 50% in early 2015 to about 90% or better today for all major platforms except Linux, which sits at 77%. This has presented huge concern for organizations from cyber security point of view. To detect any threats in encrypted traffic, organizations often use Transport Layer Security (TLS) inspection. TLS inspection decrypts TLS traffic, enabling security tools to look for malware and other threats, then re-encrypt the session. This, of course, presents new risks because the traffic is in the clear, unencrypted form during the inspection process - user privacy is compromised.

In the future, FE can be used for VPN, and specific computing key(s) can be used by security tool(s) for such inspection while VPN content remains to be encrypted/protected – no privacy compromise.

4 PET Adoption and Barriers

While a lot of research work and "proof of concept" trials have been done for different PETs, large scale adoption has not been widely deployed in actual business. There are number of reasons. Here are our observations:

- The common perception in the industry is that cryptographic technology needs to be part of the NIST standard portfolio to be considered secure. While there is an on-going PEC project within NIST, hardly any PET is part of NIST standard yet.
- In fact, data privacy regulations such as HIPAA do not provide clear requirements for data protection technology, and they are sometime conflicting. We recently conducted a study in this area. Such study is time consuming and very costly.
- To avoid such confusion, consistent and more clarity of regulations will certainly help. Moreover, regulations should provide a clear path to allow continued technological innovation.
- We all agree that it would be beneficial to have a common reference to guide business/government agencies about specific type of PET that is ready for production. If NIST standard is the one, current NIST standard process might not serve the needs with multi-year timeline. Furthermore, resource constraint might put things into queue before such technology can be put on the starting line of standardization.
- Lastly, it would be good to recognize the fact that different PET might be at different maturity stage. Based on maturity stage, different actions need to be prioritized to speed up research, adoption, and deployment. For example,
    - for technologies such as ABE that are mature and ready for production deployment, the urgent action is to speed up any needed standardization or deployment guideline as well as to provide clarity about its ability to support regulatory compliance.
    - For technologies that require more research and enhancements, proper government funding and policy will accelerate the speed to achieve maturity.

5 Conclusion

NTT Research appreciates OSTP taking a leadership position in advancing PET. We are honor to provide you with our inputs. We welcome any follow-up opportunity to support this initiative.

References

[i] Amit Sahai and Brent Waters – “Fuzzy Identity-Based Encryption”: https://eprint.iacr.org/2004/086

[ii] NIST Special Publication 800-162 – “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[iii] Boneh, Dan; Amit Sahai; Brent Waters – “Functional Encryption: Definitions and Challenges”: https://eprint.iacr.org/2010/543.pdf

[iv] Giovanni Bartolomeo – “Attribute-Based Encryption for Access Control in Cloud Ecosystems”: https://www.techrxiv.org/articles/preprint/Attribute-Based_Encryption_for_Access_Control_in_Cloud_Ecosystems/13546871

[v] Google Transparency Report - https://transparencyreport.google.com/https/overview?hl=e