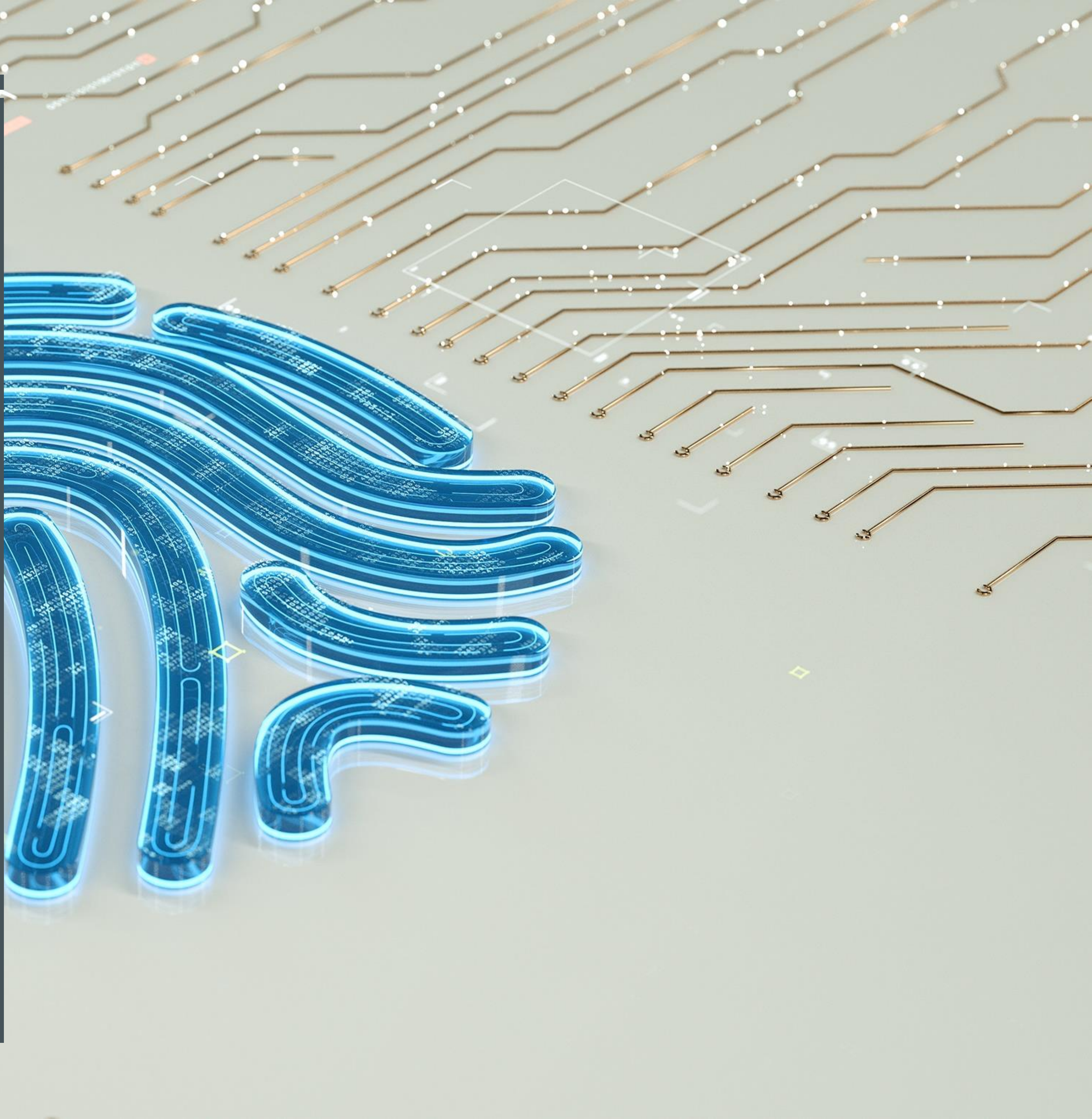
VERIFIABLE CREDENTIALS

Credential Technology Roadmap – World Wide Web Consortium (W3C)

GRAYE HOLDER, LEAD ENGINEER

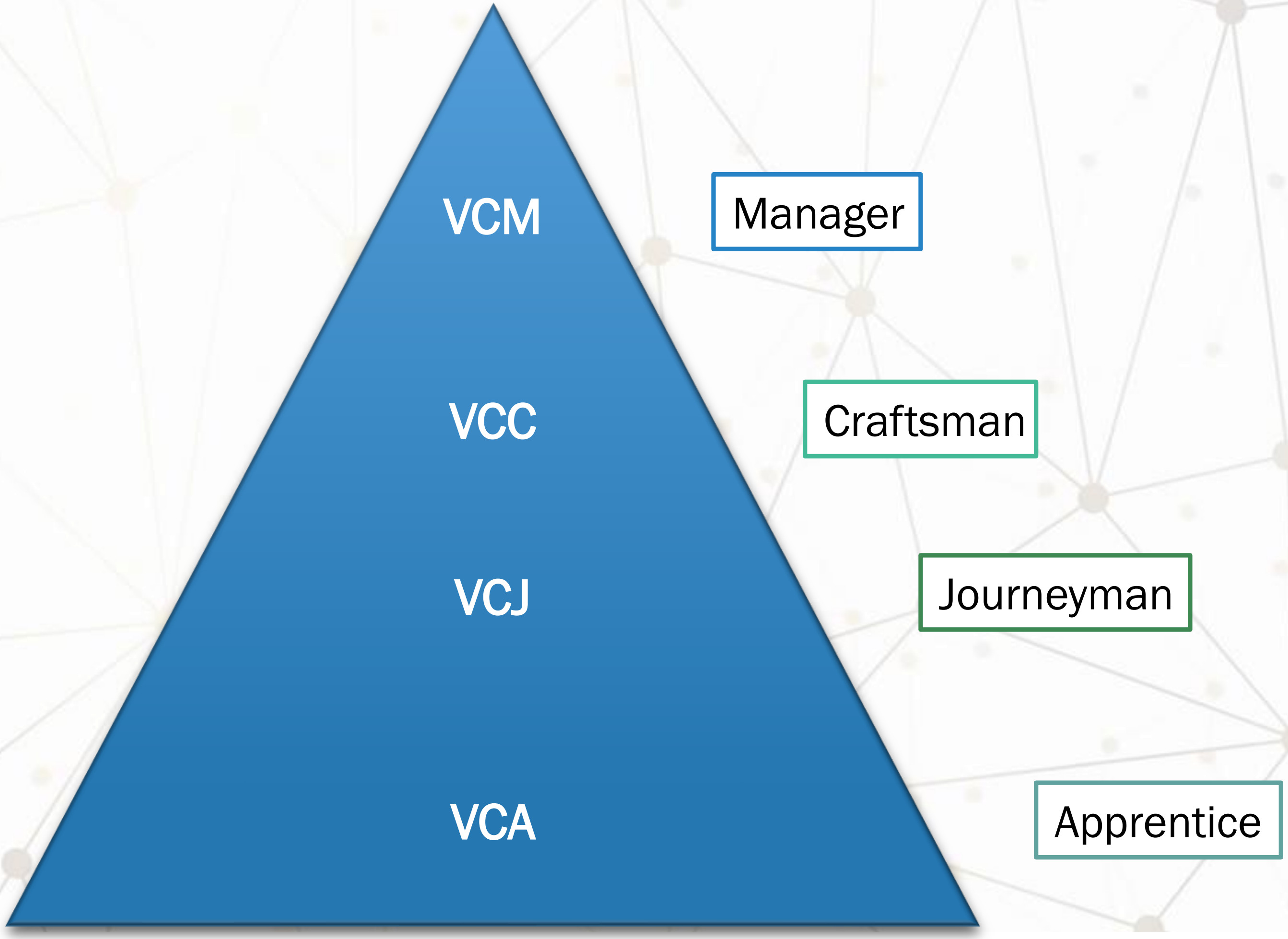
19 JAN 2022



AIR FORCE PKI SYSTEMS PROGRAM OFFICE

- So, you want to be a United States Air Force Verifiable Credential Manager?
- Hands On
- What Is Verifiable Credential
- How do I get a Verifiable Credential
- How do I use a Verifiable Credential

UNITED STATES AIR FORCE VERIFIABLE CREDENTIAL EXPERT LEVELS



VCM

Manager

VCC

Craftsman

VCJ

Journeyman

VCA

Apprentice

OBJECTIVE

- The objective of this session is for attendees to comprehend W3C Verifiable Credentials

SAMPLES OF BEHAVIOR

- Define the W3C Verifiable Credential (VC)
- Define the W3C Decentralized Identifier (DID)
- Identify the properties of a Verifiable Credential
- Compare and Contrast Verifiable Credentials to other Credentials
- Explain how Verifiable Credentials may impact USAF ICAM Programs and Systems
- Draw a basic verifiable credential architecture
- Using a digital wallet show and explain how a verifiable credential is issued, protected, and verified
- Define a Non-Fungible Token (NFT)
- Using a digital wallet show and explain how an NFT is issued, protected and stored
- Value the use and security a Verifiable Credential provides

HOW DO I OBTAIN MY VERIFIABLE CREDENTIAL APPRENTICE CERTIFICATE?

Air Force Form 1256 – Certificate of Training (Apprentice Level)

- Draw a Basic Verifiable Credential Architecture Diagram take picture and send to @Graye Holder in Mattermost and state you have the tools needed installed on a mobile device
- Tools Needed
  - Microsoft Authenticator – Verifiable Credentials
  - WallaWallet – Hedera TestNet xfer of 1 Hbars from 0.0.15844788 with timestamp and note that account holder has a completed certificate good for 3 years from timestamp
- Hedera Token Service (HTS) – Future concept
- Hedera issued NFT when available from WallaWallet – Future concept

Future – ION Network and Hedera Network NFTs (Journeyman Level)

- HTS – Tokens and NFTs
- Hedera Consensus Service – Future Topic
- Decentralized Identifiers
- Non-Fungible Tokens

OVERVIEW

COVID-19 Test for Virus: 02 JUL 2020

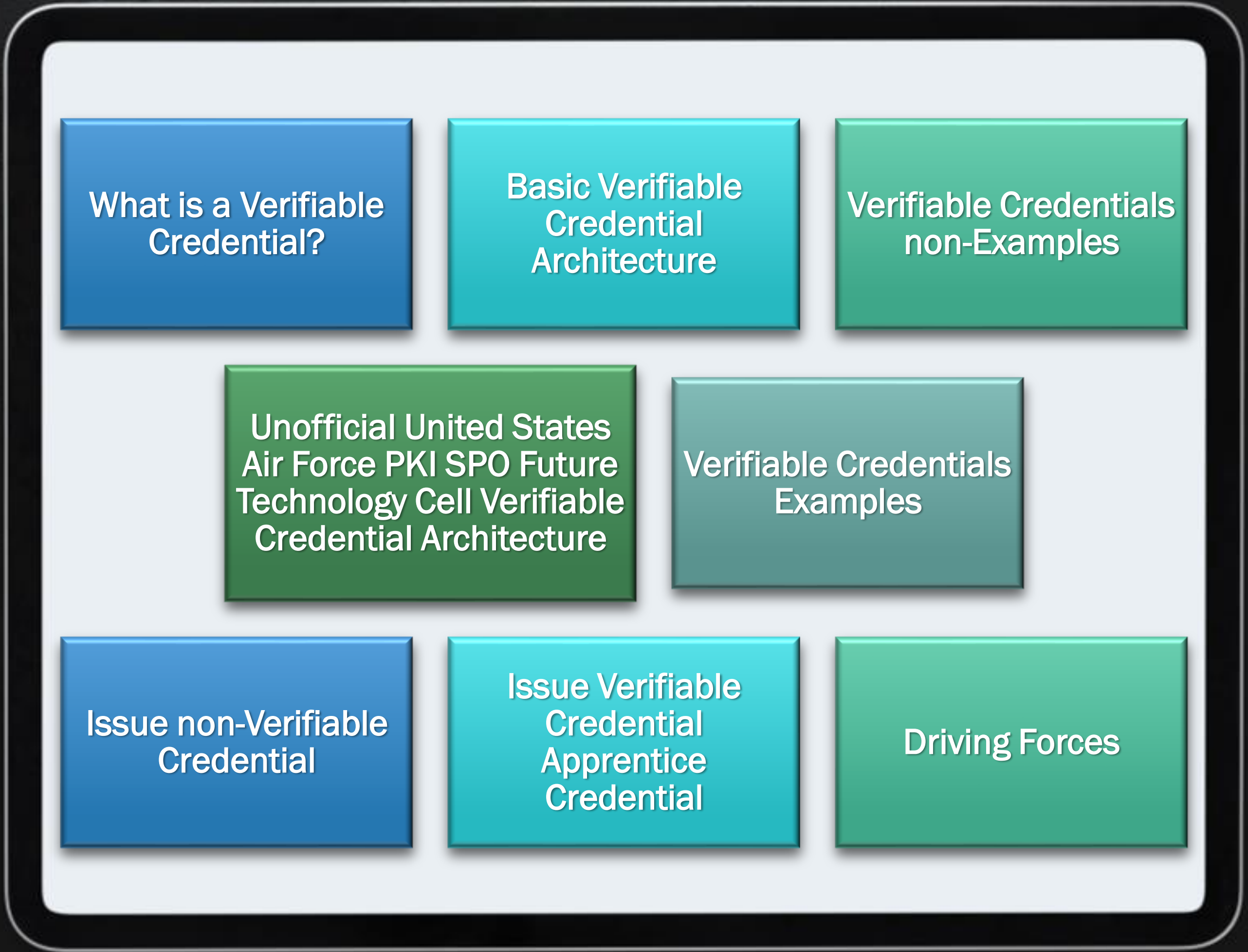
Show QR code

Melissa Peterson

Test type:	Test for Virus
Test result:	COVID-19 virus NOT detected
Test date:	10:51 on 02 JUL 2020
Test name:	FRANKD COVID-19 Real-time RT-PCR
Test reliability:	Sensitivity: 100% Specificity: 100%
Approval type:	
Tested at:	Geneme In Vitro Diagnostic Device

View full test details >

View previous test results >



What is a Verifiable Credential?

Basic Verifiable Credential Architecture

Verifiable Credentials non-Examples

Unofficial United States Air Force PKI SPO Future Technology Cell Verifiable Credential Architecture

Verifiable Credentials Examples

Issue non-Verifiable Credential

Issue Verifiable Credential Apprentice Credential

Driving Forces

WHAT IS A VERIFIABLE CREDENTIAL?

- A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects.

Ref: W3C Verifiable Credential Data Model V1.1, 9 Nov 2021

- Verifiable Credential Properties
  - Much like a physical credential
  - They cannot be copied
  - Extremely hard to steal
  - Privacy protecting
  - Support least privileges / authority
  - Cost virtually nothing to issue
  - Don’t need multiple cards
  - Ability to delegate (based on governance)

Ref: Self Sovereign Identity

WHAT IS A W3C DENCENTRALIZED IDENTIFIER (DID)

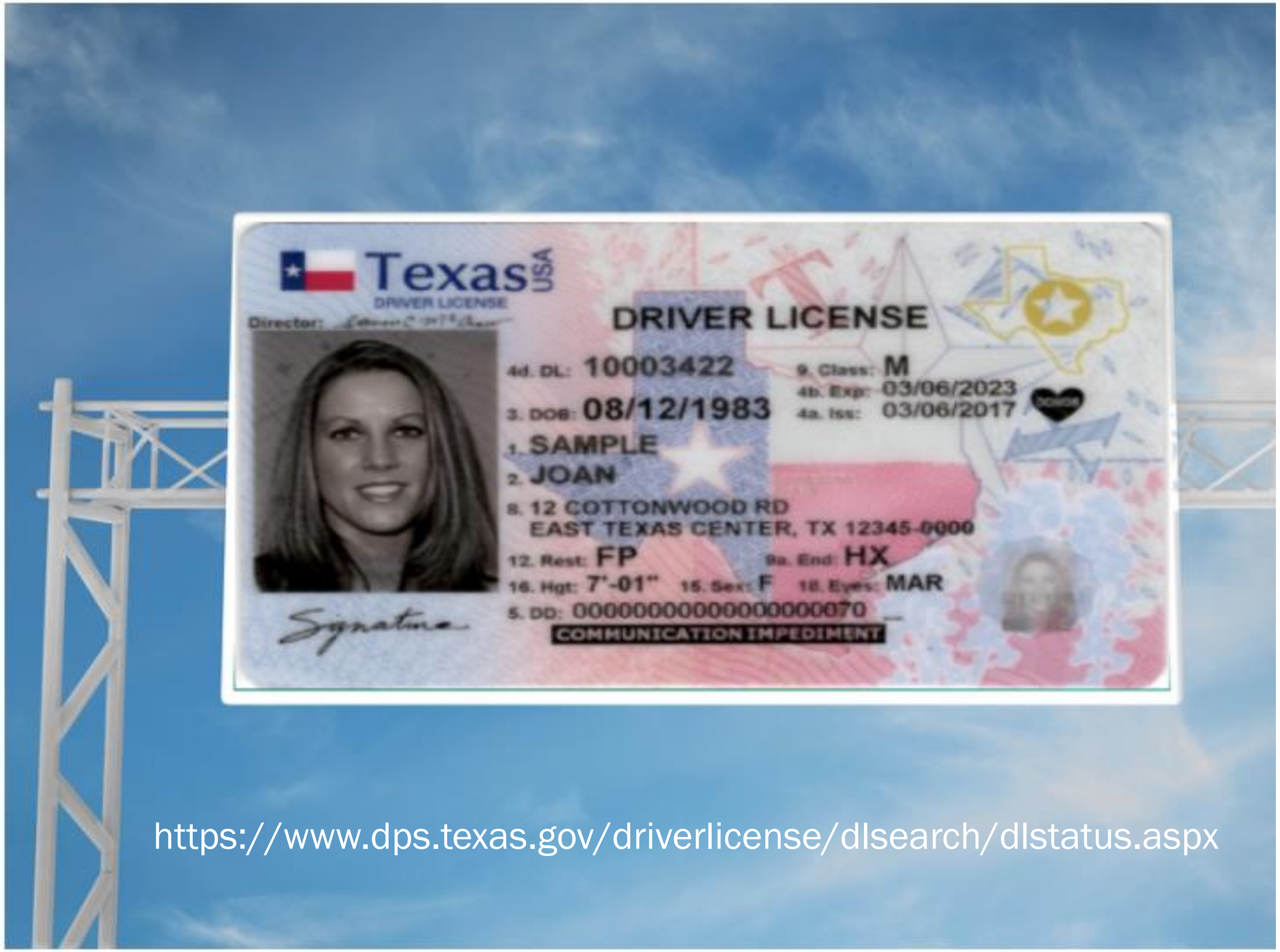
A new type of globally unique identifier: a string of characters that identify a resource.

Example: instead of http:// or https:// or ftp:// a did is typically identified as: did: such as the did used in this demonstration did:ion

- DID Properties / Goals
  - Ease of creation
  - Decentralized
  - Persistent
  - Resolvable
  - Cryptographically Verifiable

VERIFIABLE CREDENTIAL - NON-EXAMPLE 1

Drivers License



Texas USA
DRIVER LICENSE
Director:

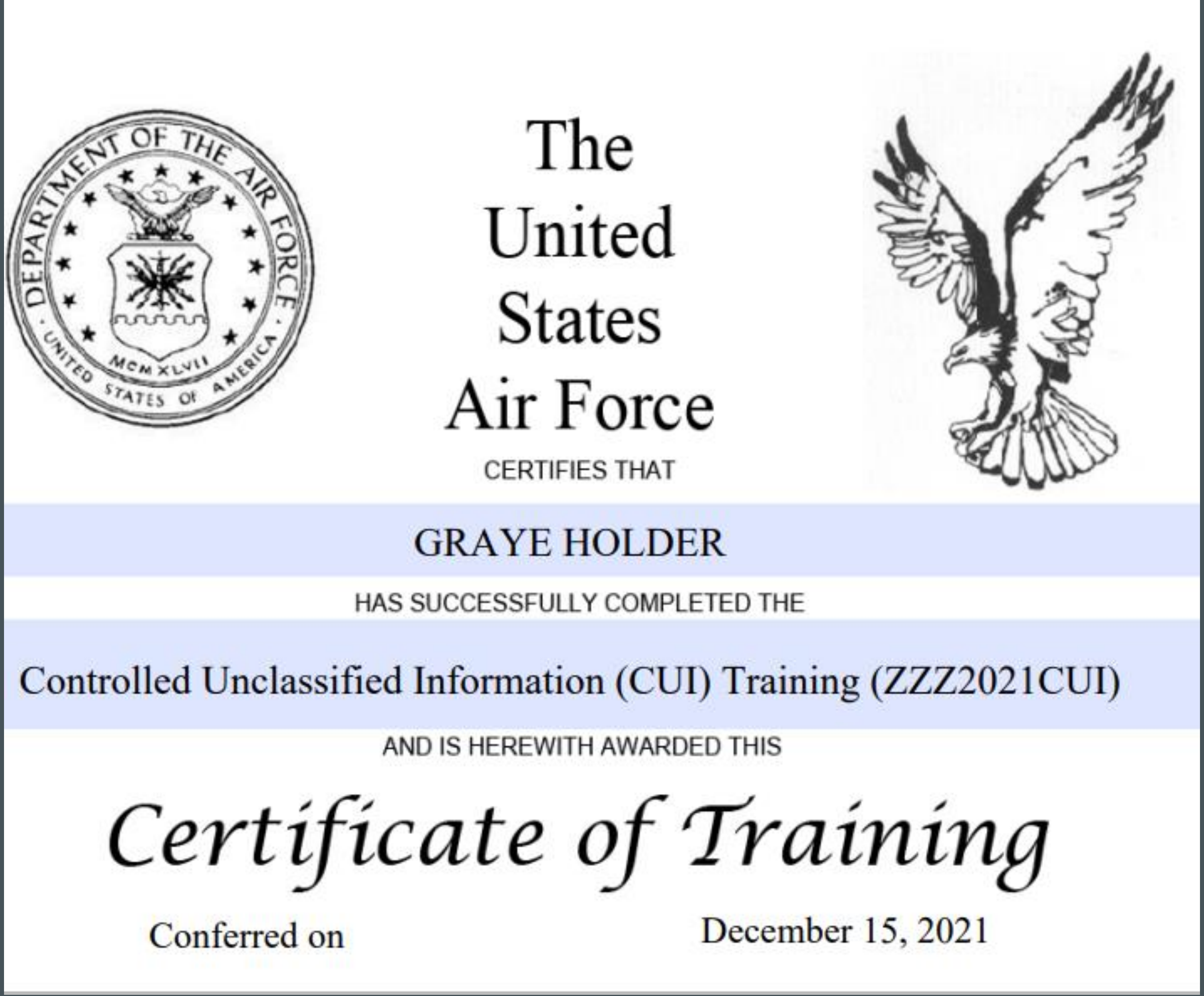
DRIVER LICENSE

4d. DL: 10003422
9. Class: M
4b. Exp: 03/06/2023
3. DOB: 08/12/1983
4a. Iss: 03/06/2017
1. SAMPLE
2. JOAN
8. 12 COTTONWOOD RD
EAST TEXAS CENTER, TX 12345-0000
12. Rest: FP
9a. End: HX
16. Hgt: 7'-01"
15. Sex: F
18. Eyes: MAR
5. DD: 00000000000000000000070
COMMUNICATION IMPEDIMENT

Signature

https://www.dps.texas.gov/driverlicense/dlsearch/dlstatus.aspx

VERIFIABLE CREDENTIAL – NON-EXAMPLE 2



DEPARTMENT OF THE AIR FORCE

MCMXLVII

UNITED STATES OF AMERICA

The
United
States
Air Force

CERTIFIES THAT

GRAYE HOLDER

HAS SUCCESSFULLY COMPLETED THE

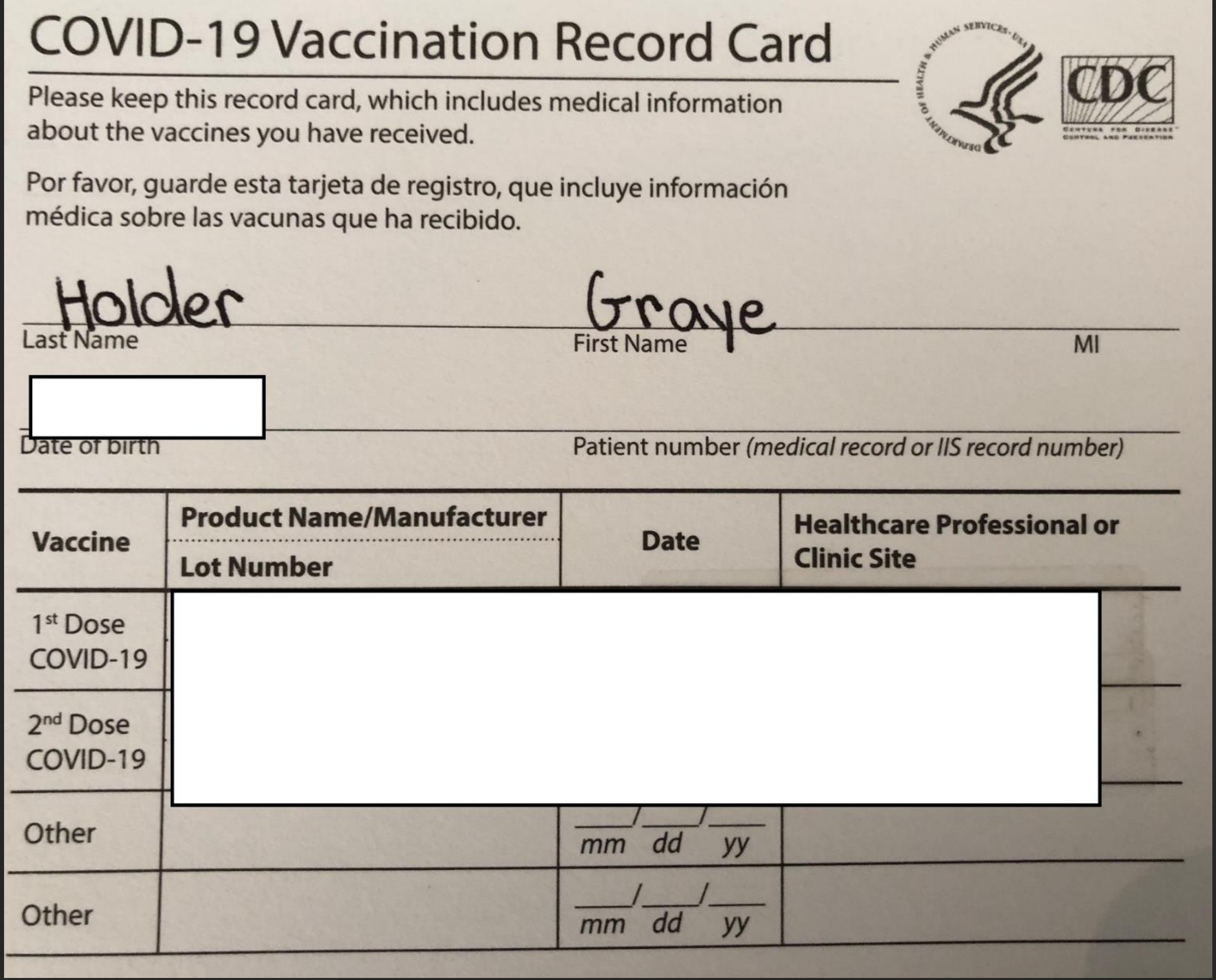
Controlled Unclassified Information (CUI) Training (ZZZ2021CUI)

AND IS HEREWITH AWARDED THIS

Certificate of Training

Conferred on December 15, 2021

VERIFIABLE CREDENTIAL – NON-EXAMPLE 3



COVID-19 Vaccination Record Card

Please keep this record card, which includes medical information about the vaccines you have received.

Por favor, guarde esta tarjeta de registro, que incluye información médica sobre las vacunas que ha recibido.

Holder
Last Name

Graye
First Name

MI

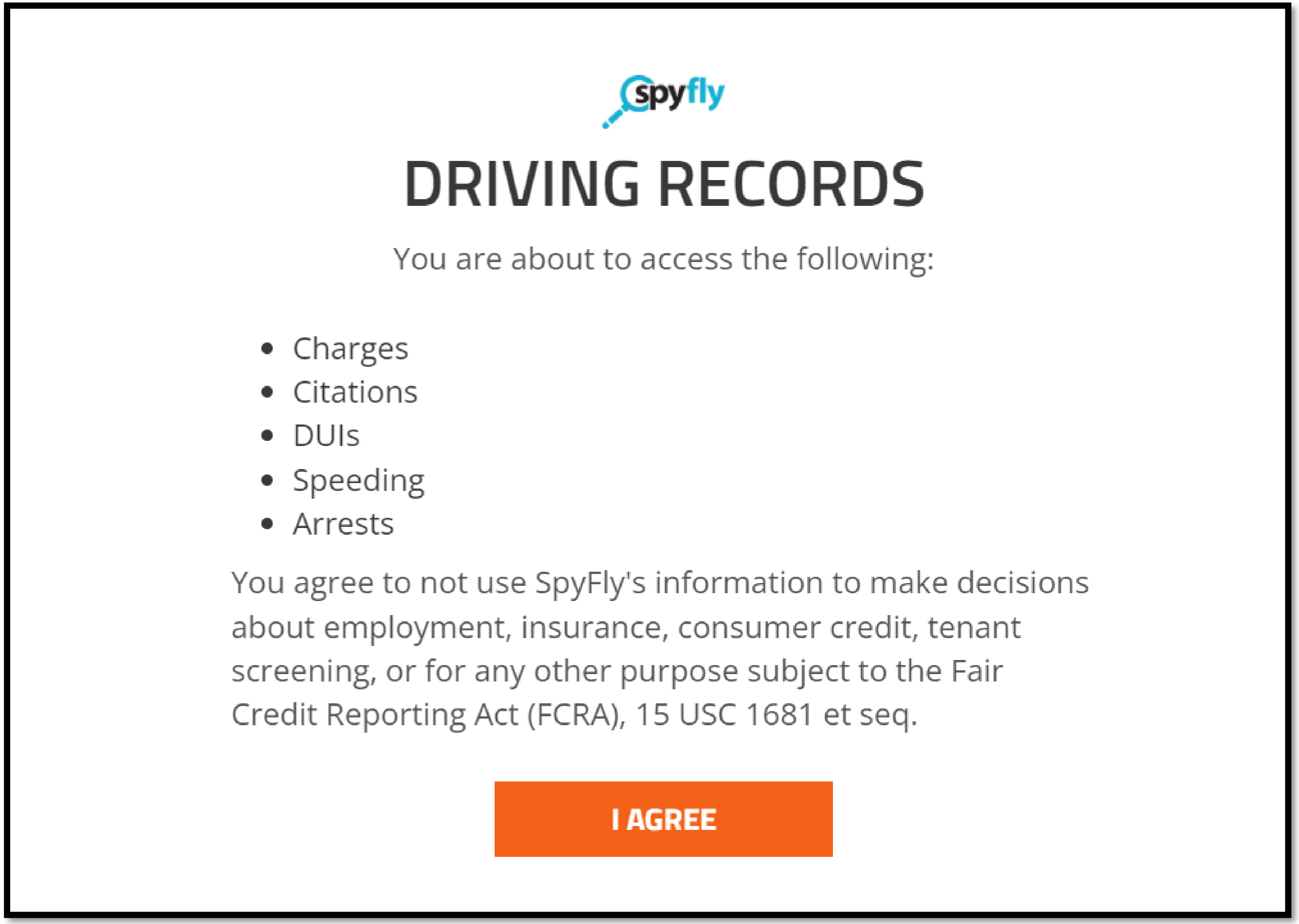
[redacted]
Date of birth

Patient number *(medical record or IIS record number)*

Vaccine	Product Name/Manufacturer Lot Number	Date	Healthcare Professional or Clinic Site
1st Dose COVID-19	[redacted]	[redacted]	[redacted]
2nd Dose COVID-19	[redacted]	[redacted]	[redacted]
Other		___/___/___ mm dd yy	
Other		___/___/___ mm dd yy	

VERIFIABLE CREDENTIAL – NON-EXAMPLE 4

Public – Verifiable Data Registry



DRIVING RECORDS

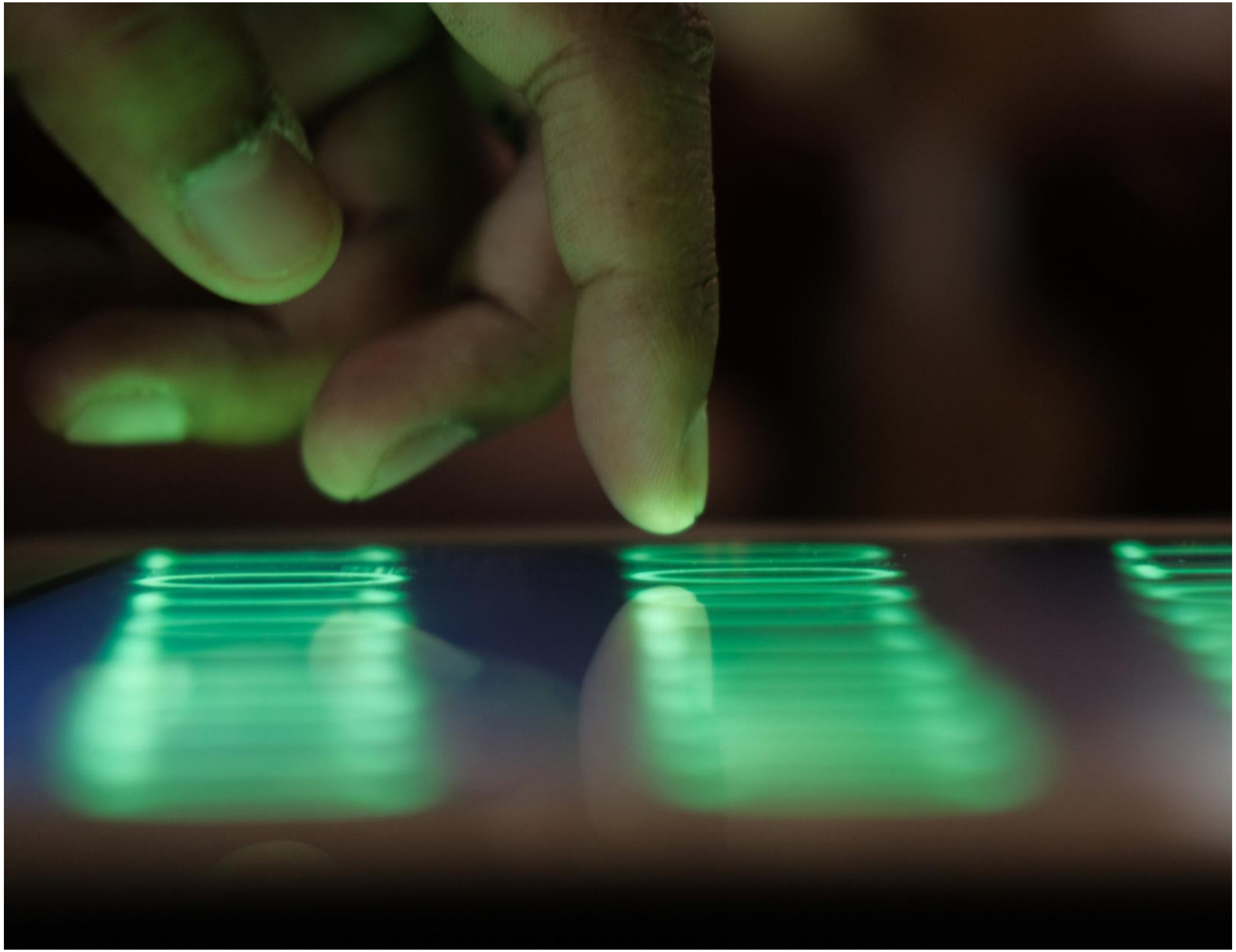
You are about to access the following:

- Charges
- Citations
- DUIs
- Speeding
- Arrests

You agree to not use SpyFly's information to make decisions about employment, insurance, consumer credit, tenant screening, or for any other purpose subject to the Fair Credit Reporting Act (FCRA), 15 USC 1681 et seq.

VERIFIABLE CREDENTIAL – NON-EXAMPLES

- Tamper-evident credential
- Have authorship cryptographically verified
- Built verifiable presentations
- The claims in a credential can be about different subjects



PIV X.509 AUTHENTICATION CERTIFICATE

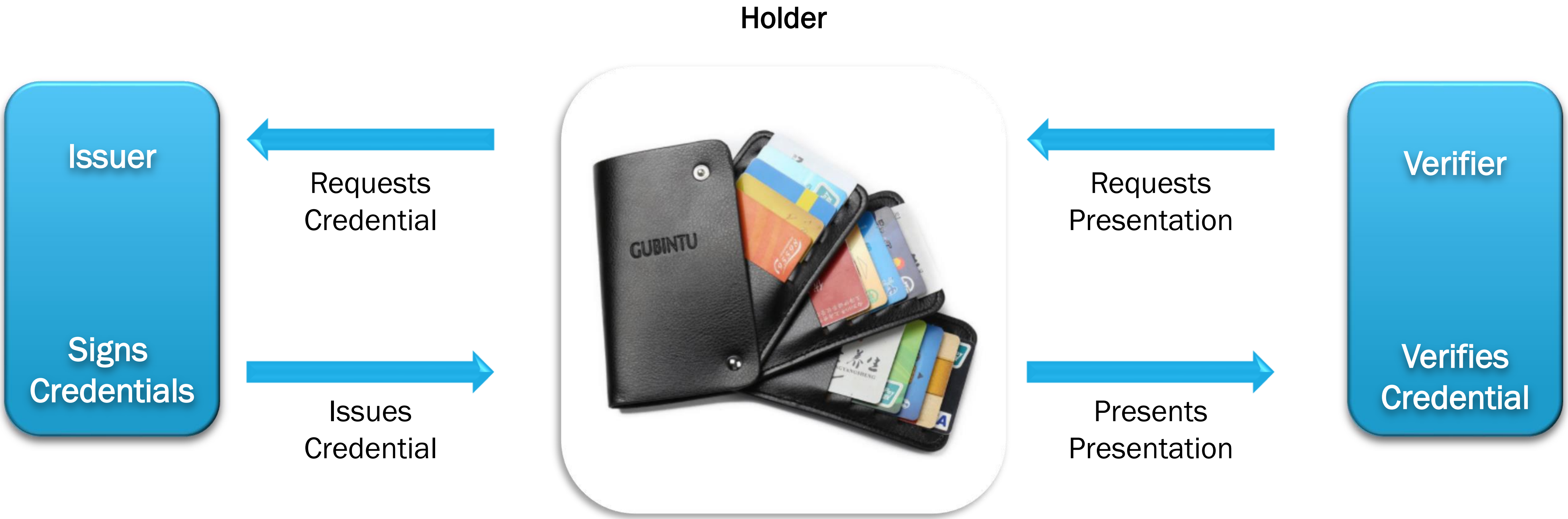
- A set of one or more claims made by an issuer; A ***verifiable credential*** is a tamper-evident credential that has authorship that can be cryptographically verified
- Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified
- The claims in a credential can be about different subjects

Credential Attributes	Has Credential Property
Claims made by an issuer	Yes
Data structure that authoritatively binds a digital identity	Yes
One or more identifiers	Yes
To at least one authenticator controlled by entity with the digital identity	Yes

W3C VERIFIABLE CREDENTIAL VS X.509 PKI CERTIFICATE

Verifiable Credential Property	Has VC Property
Much like a physical credential	No
They cannot be copied	No
Extremely hard to steal	No
Privacy protecting	No
Support least privileges / authority	No
Cost virtually nothing to issue	Yes and No
Don’t need multiple cards	No
Ability to delegate (based on governance)	No

VERIFIABLE CREDENTIAL – WHAT DOES IT LOOK LIKE



Holder

Issuer

Signs Credentials

Requests Credential

Issues Credential

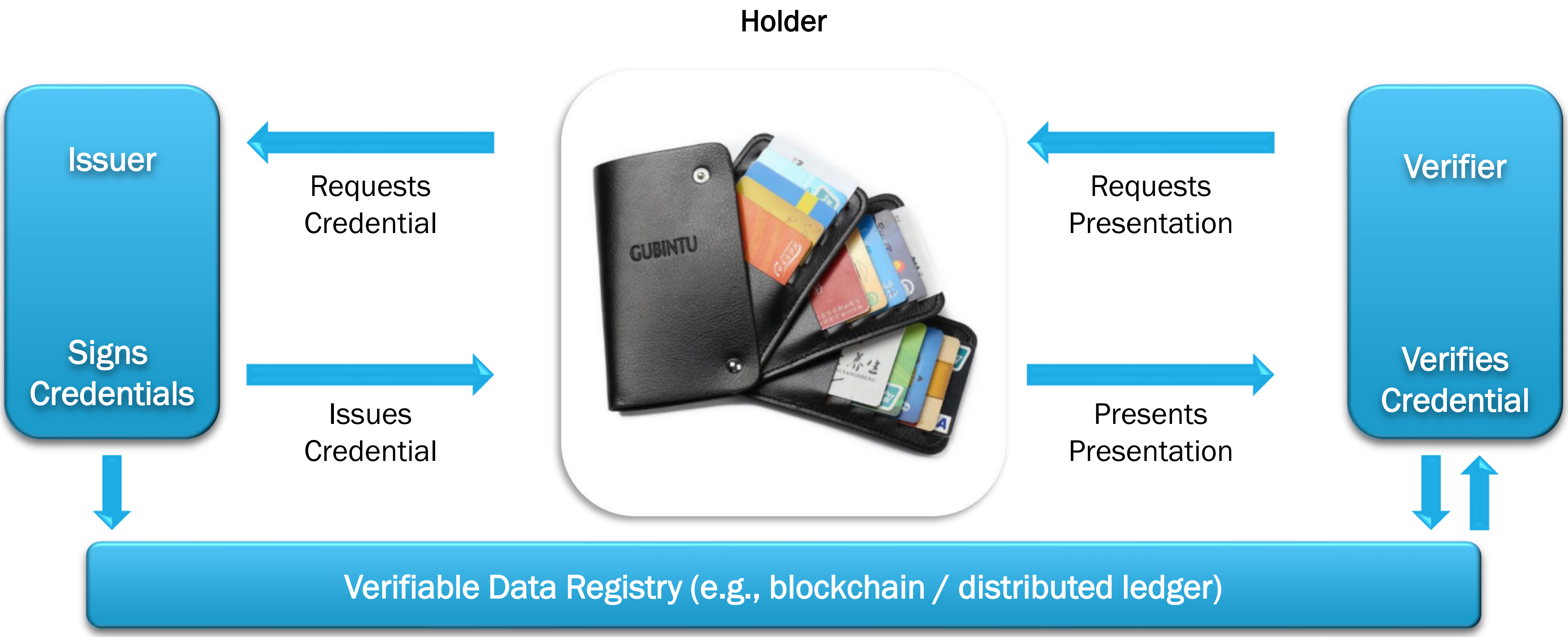
Requests Presentation

Presents Presentation

Verifier

Verifies Credential

VERIFIABLE CREDENTIAL – WHAT MAKES IT POSSIBLE



Holder

Issuer

Signs Credentials

Requests Credential

Issues Credential

Requests Presentation

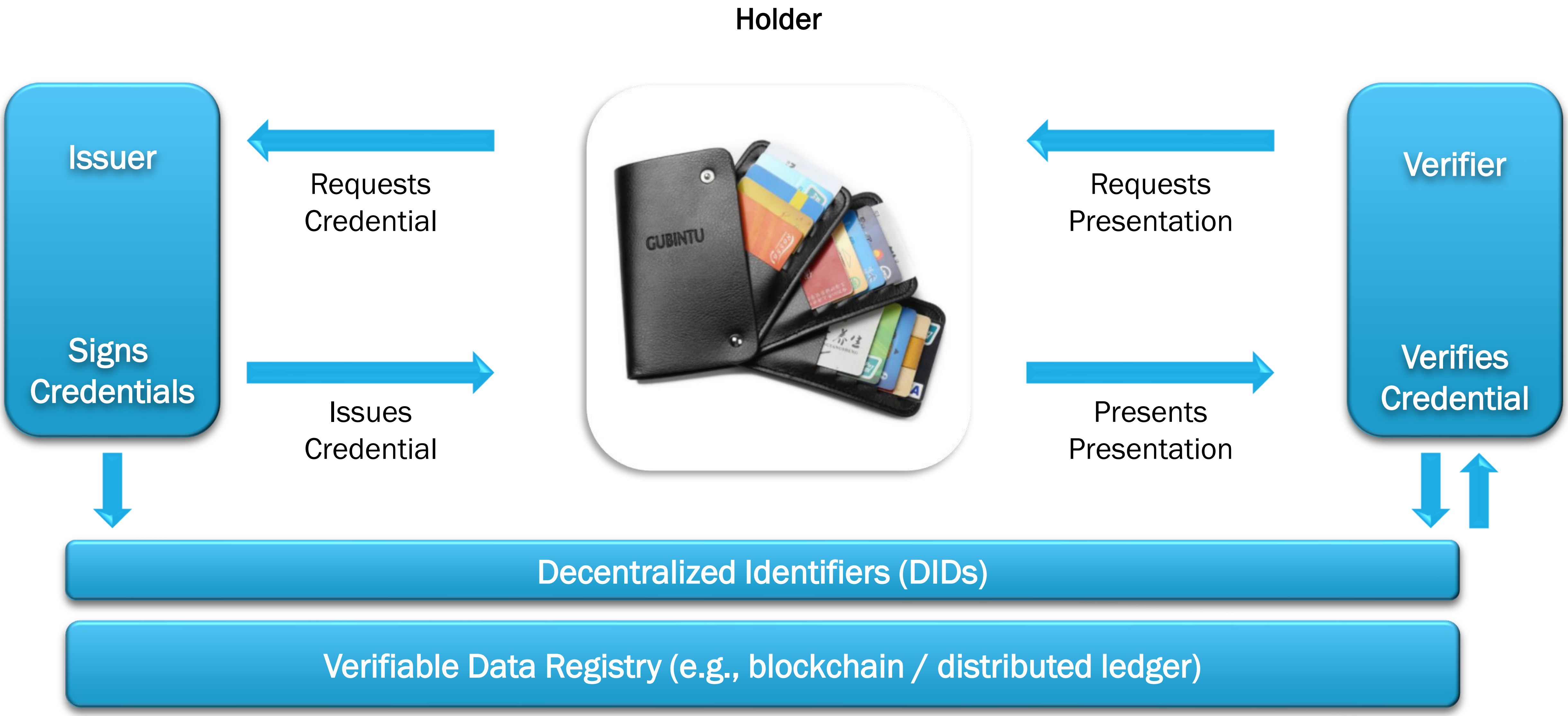
Presents Presentation

Verifier

Verifies Credential

Verifiable Data Registry (e.g., blockchain / distributed ledger)

BASIC VERIFIABLE CREDENTIAL ARCHITECTURE



Holder

Issuer

Signs Credentials

Requests Credential

Issues Credential

Requests Presentation

Presents Presentation

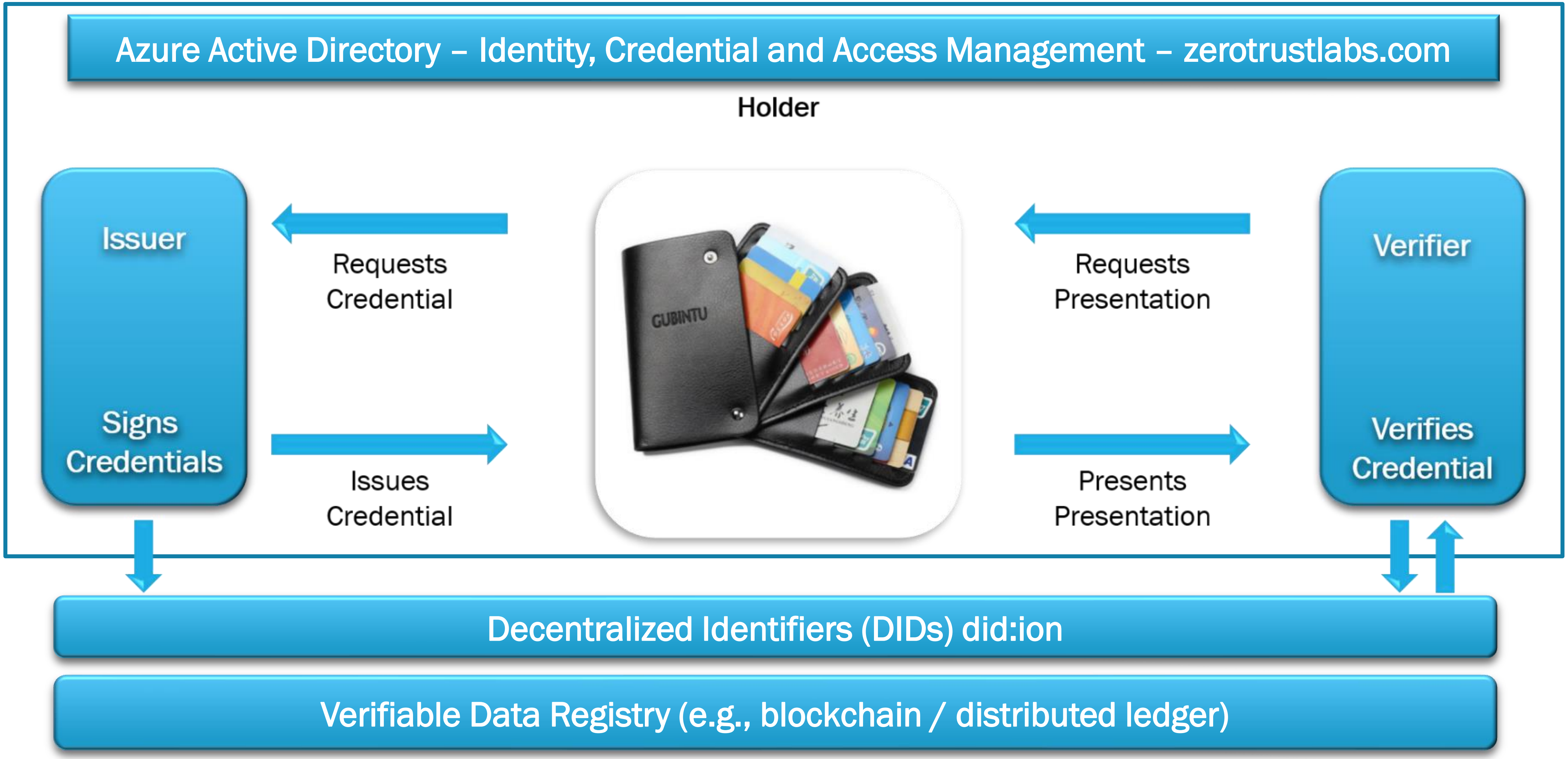
Verifier

Verifies Credential

Decentralized Identifiers (DIDs)

Verifiable Data Registry (e.g., blockchain / distributed ledger)

UNOFFICIAL UNITED STATES AIR FORCE PKI SPO FUTURE TECHNOLOGY CELL
WEB 3 VERIFIABLE CREDENTIAL ARCHITECTURE



Azure Active Directory – Identity, Credential and Access Management – zerotrustlabs.com

Holder

Issuer

Signs Credentials

Requests Credential

Issues Credential

Requests Presentation

Presents Presentation

Verifier

Verifies Credential

Decentralized Identifiers (DIDs) did:ion

Verifiable Data Registry (e.g., blockchain / distributed ledger)

A WORD ABOUT FAST IDENTITY ONLINE (FIDO)

Why FIDO – Device-centric authentication – wallets (public private) kept on and interaction with device will send identity related signal to verifier that transaction is authorized

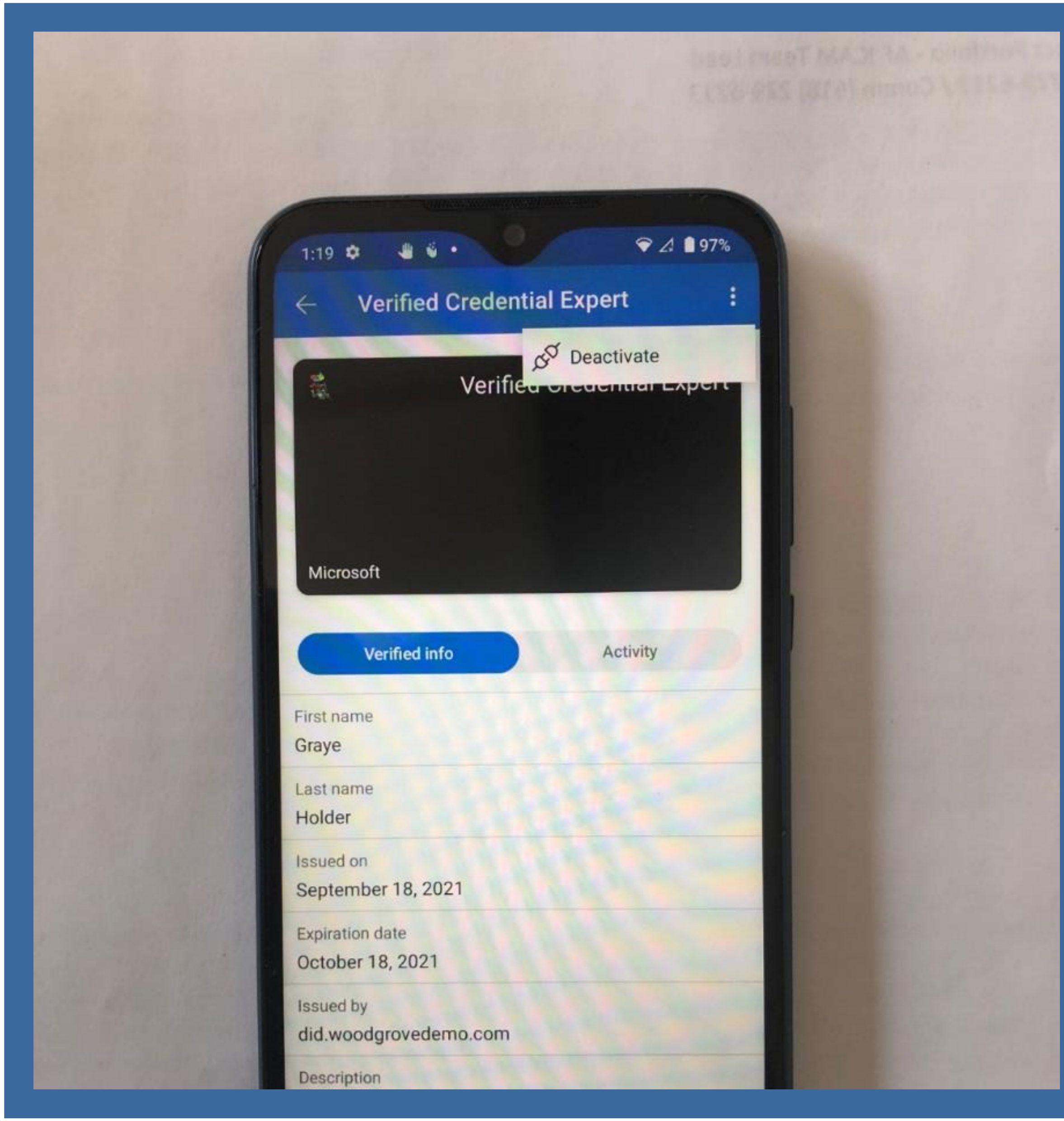
NOTE: Interaction can be human, or nonhuman based – delegated

Services now only need to make a single choice for a secure authentication user experience that is secure and easy to use

WebAuthn defines a standard web API that is being built into browsers and platforms to enable support for FIDO Authentication

DID AND DLT ARCHITECTURE COMPONENTS

- Identity Credential and Access Management System – Azure Active Directory – zerotrustlabs tenant
- Issuer – zerotrustlabs.com
- Holder – Any HNID Member
- Wallet – Microsoft Authenticator App / Credentials Beta
- Verifier – Any HNID Member or Application
- Decentralized Identifier – did:ion method
  - did:ion method
  - Issuer dids
    - woodgrovedemo.com
    - zerotrustlabs.com
- Verifiable Data Registry – sidetree
- Credential State Provider- bitcoin core



Verified Credential Expert

Verified Credential Expert

Microsoft

First name
Graye

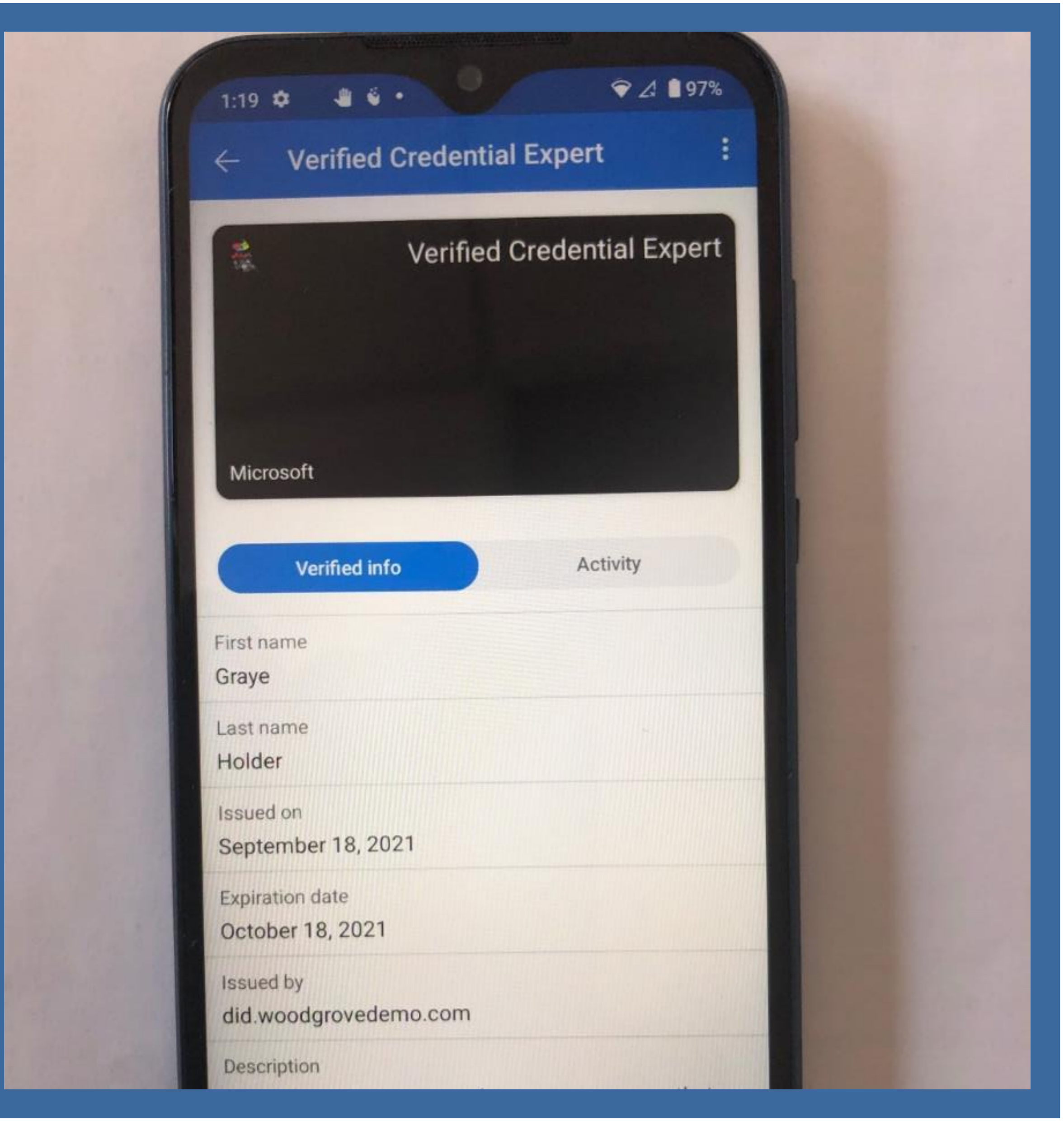
Last name
Holder

Issued on
September 18, 2021

Expiration date
October 18, 2021

Issued by
did.woodgrovedemo.com

Description



Verified Credential Expert

Verified Credential Expert

Microsoft

First name
Graye

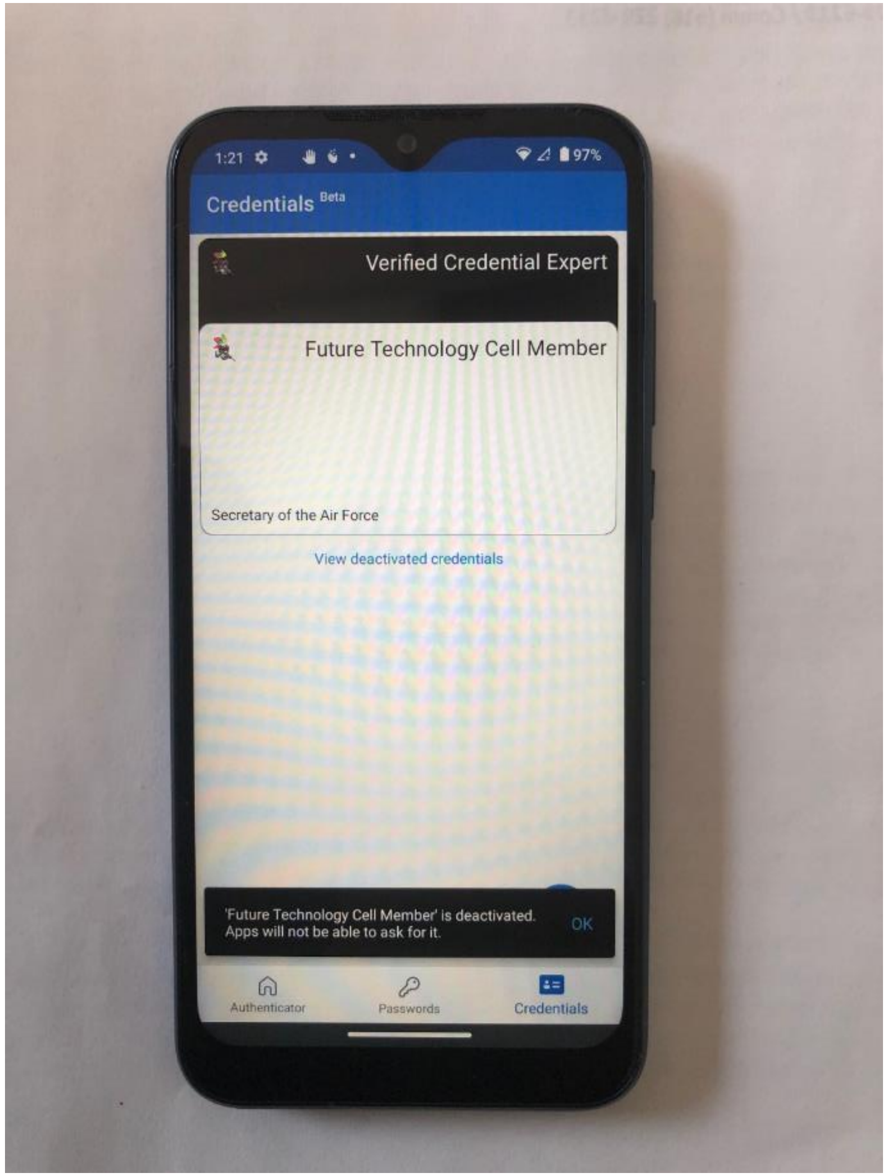
Last name
Holder

Issued on
September 18, 2021

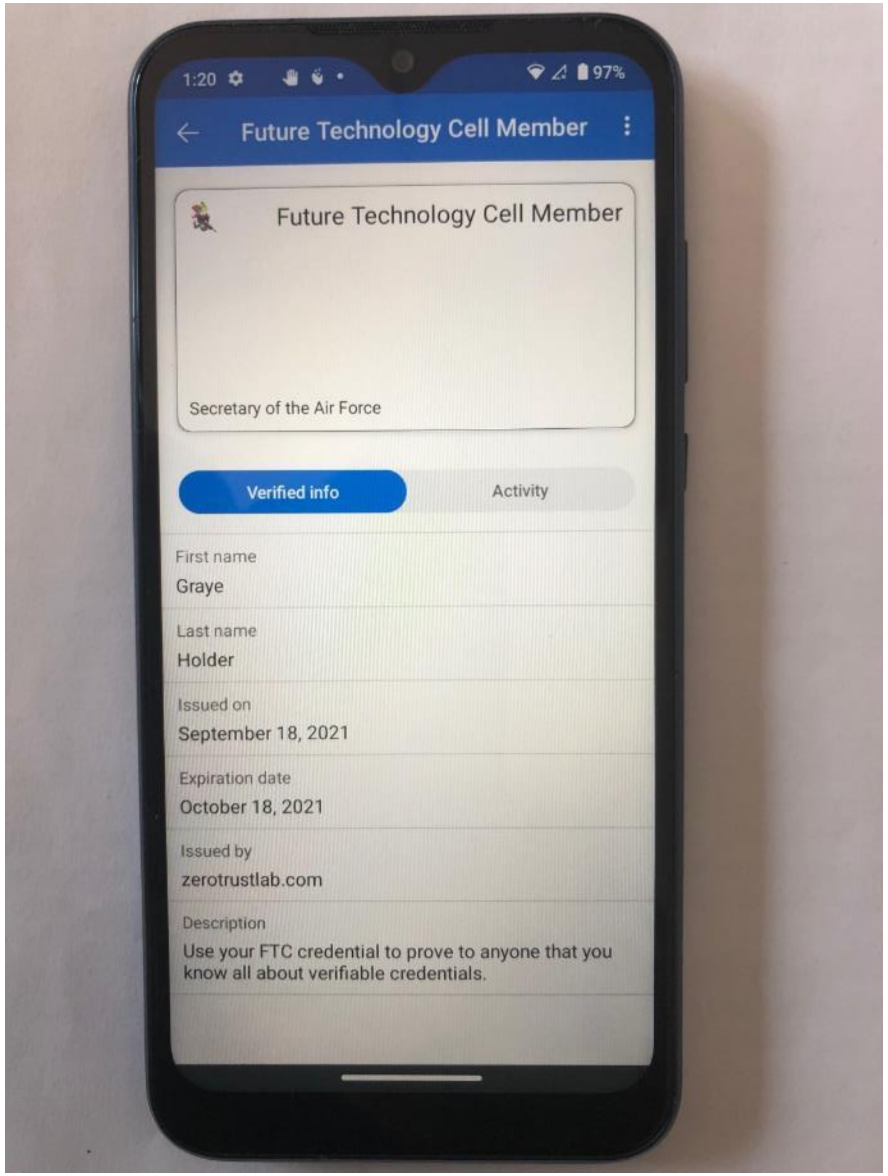
Expiration date
October 18, 2021

Issued by
did.woodgrovedemo.com

Description


1:21
97%
Credentials Beta
Verified Credential Expert
Future Technology Cell Member
Secretary of the Air Force
View deactivated credentials
OK
Authenticator
Passwords
Credentials

'Future Technology Cell Member' is deactivated. Apps will not be able to ask for it.


1:20
97%
Future Technology Cell Member
Future Technology Cell Member
Secretary of the Air Force
Verified info
Activity

First name
Graye

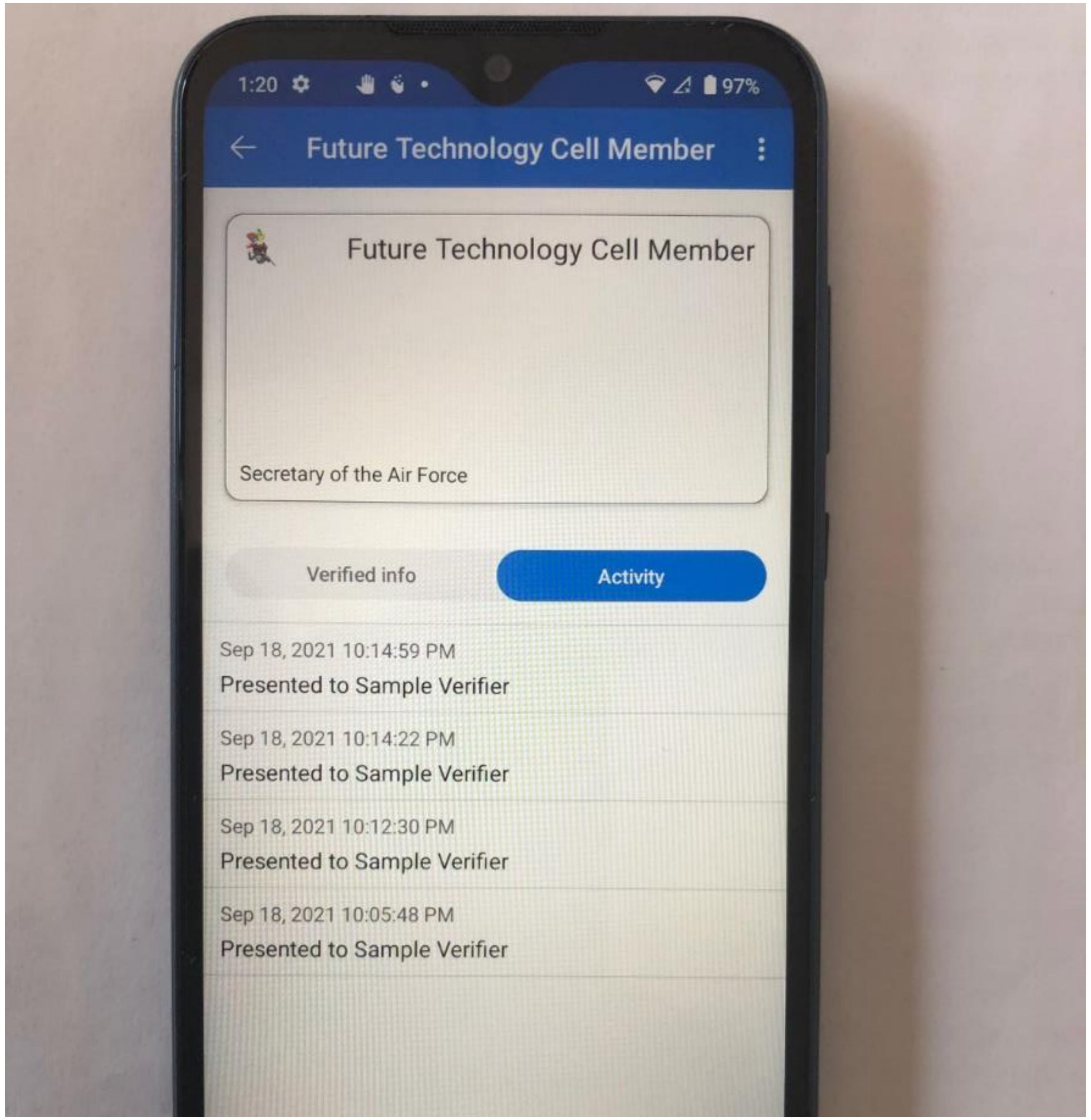
Last name
Holder

Issued on
September 18, 2021

Expiration date
October 18, 2021

Issued by
zerotrustlab.com

Description
Use your FTC credential to prove to anyone that you know all about verifiable credentials.



1:20 97%

Future Technology Cell Member

Future Technology Cell Member

Secretary of the Air Force

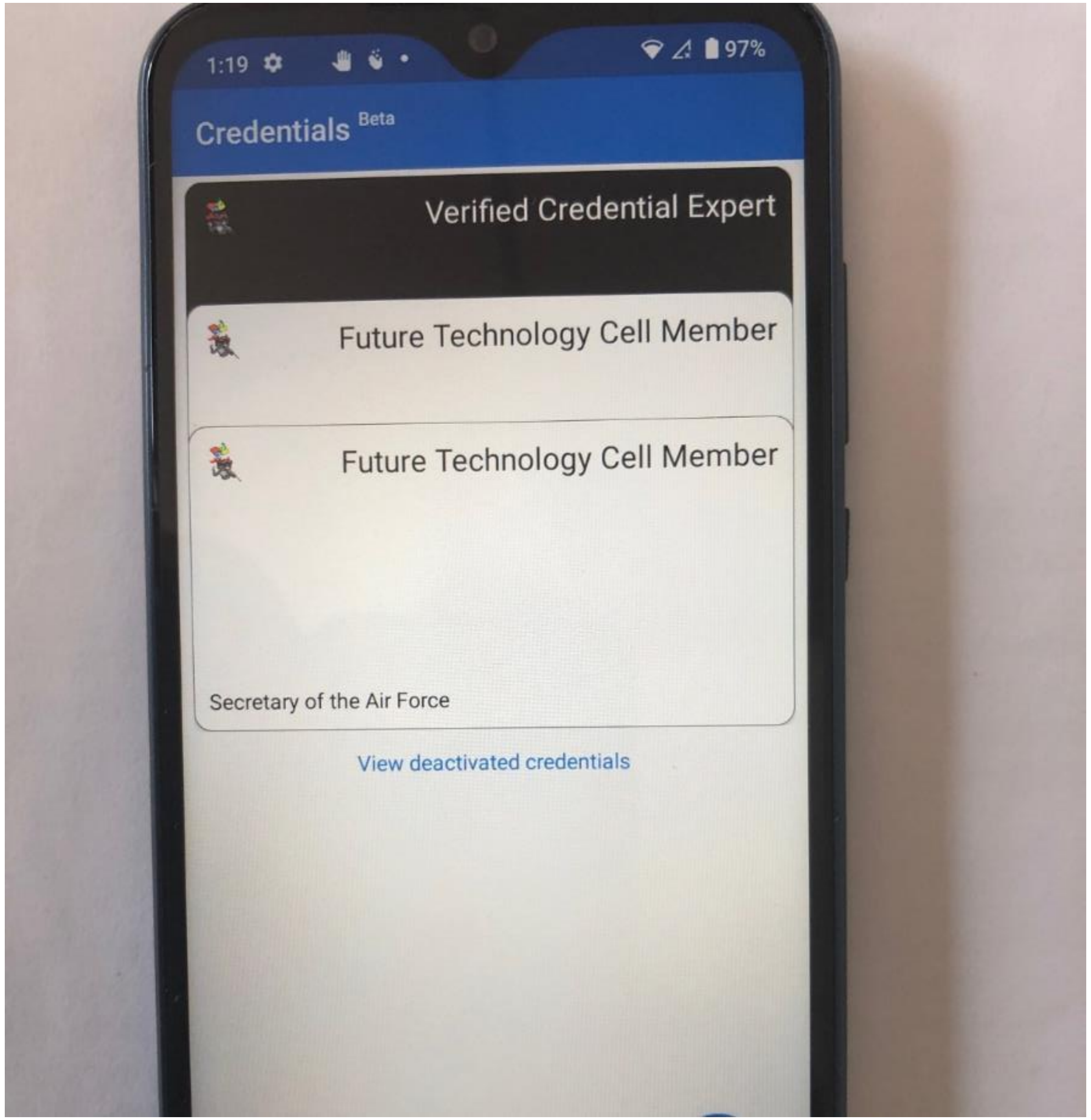
Verified info | Activity

Sep 18, 2021 10:14:59 PM
Presented to Sample Verifier

Sep 18, 2021 10:14:22 PM
Presented to Sample Verifier

Sep 18, 2021 10:12:30 PM
Presented to Sample Verifier

Sep 18, 2021 10:05:48 PM
Presented to Sample Verifier



1:19 97%

Credentials Beta

Verified Credential Expert

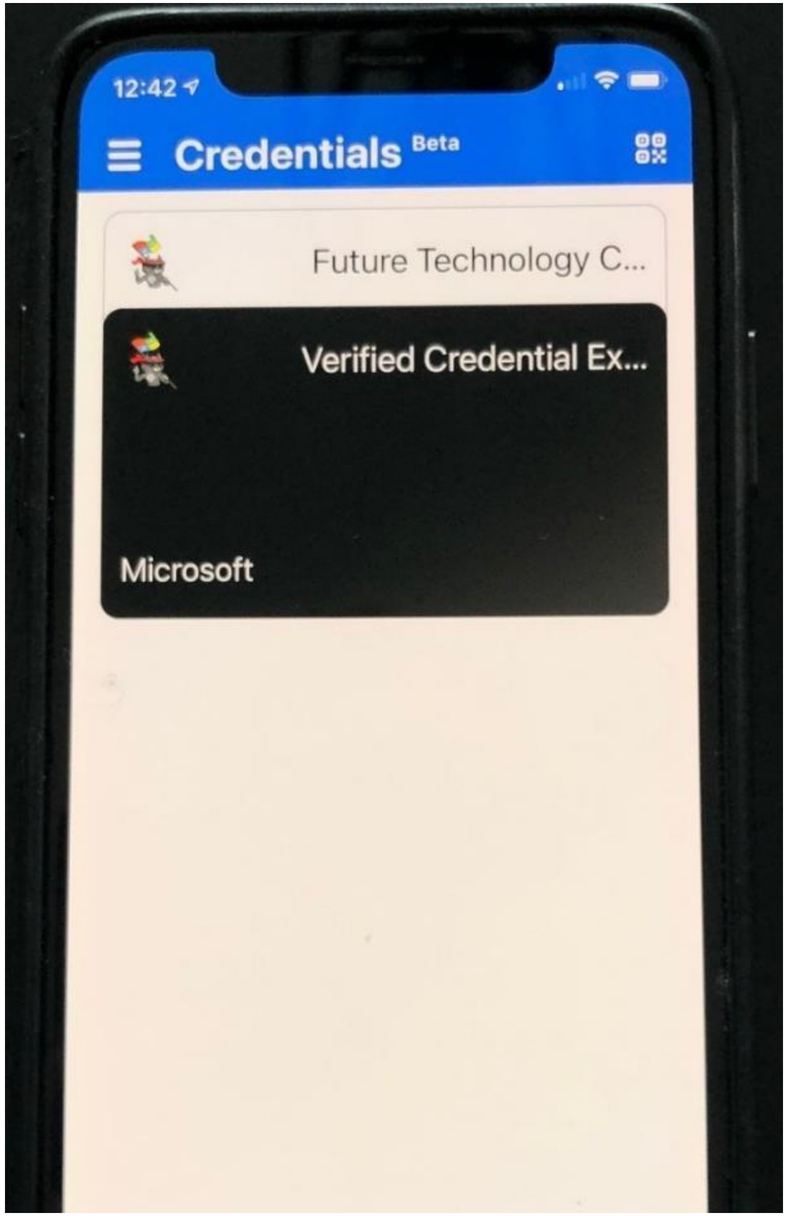
Future Technology Cell Member

Future Technology Cell Member

Secretary of the Air Force

View deactivated credentials

IOS EXPERIENCE



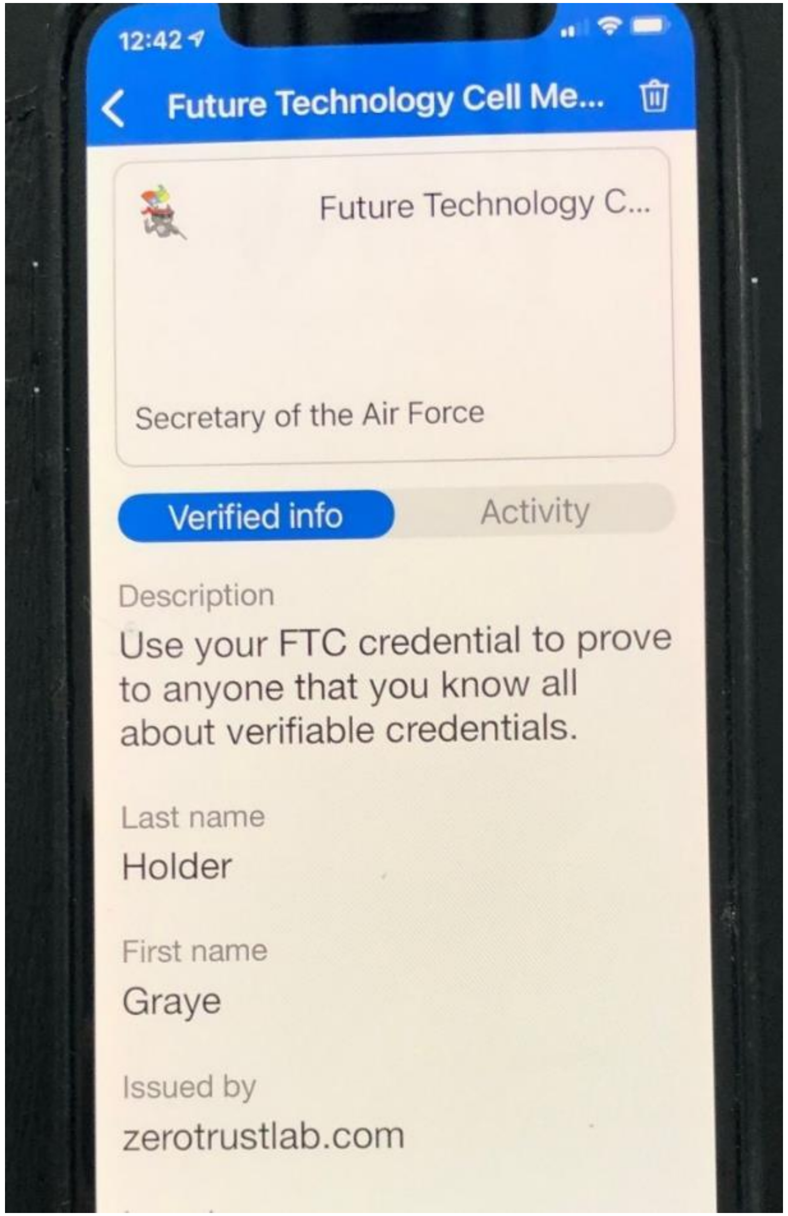
12:42

Credentials Beta

Future Technology C...

Verified Credential Ex...

Microsoft



12:42

Future Technology Cell Me...

Future Technology C...

Secretary of the Air Force

Verified info | Activity

Description

Use your FTC credential to prove to anyone that you know all about verifiable credentials.

Last name

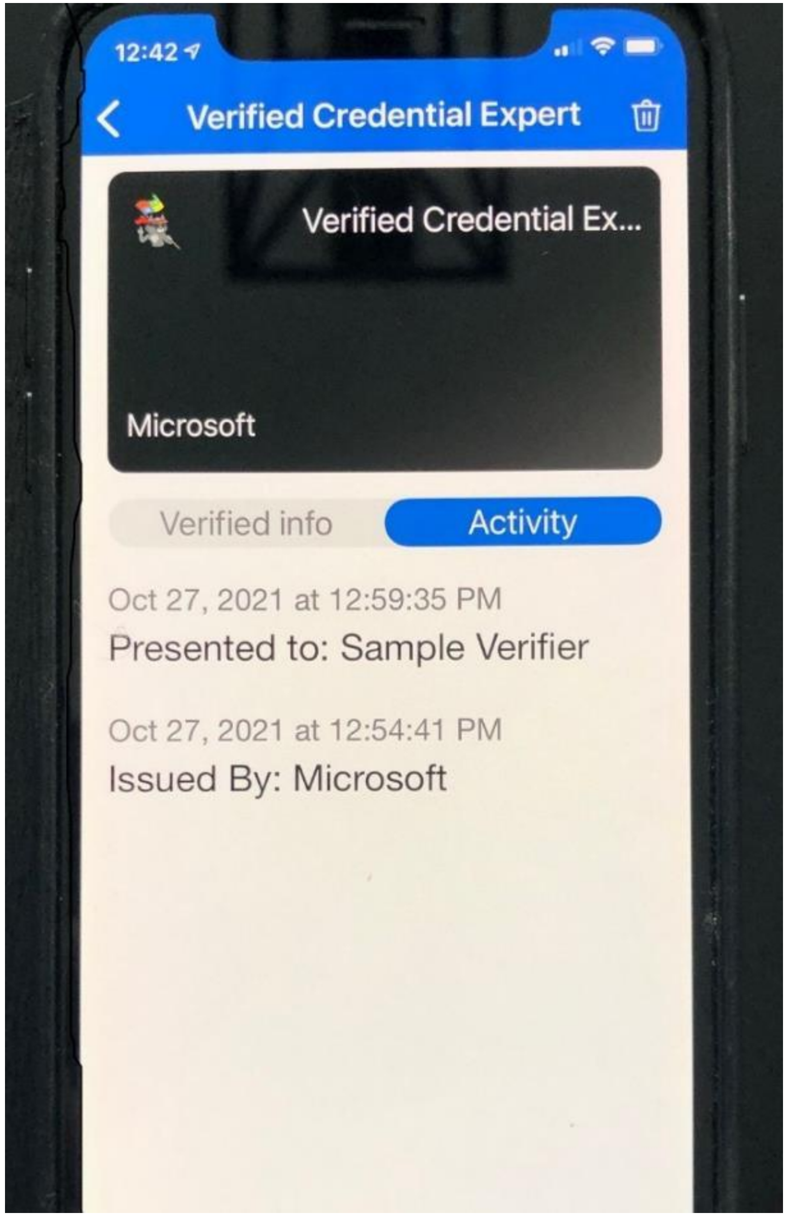
Holder

First name

Graye

Issued by

zerotrustlab.com



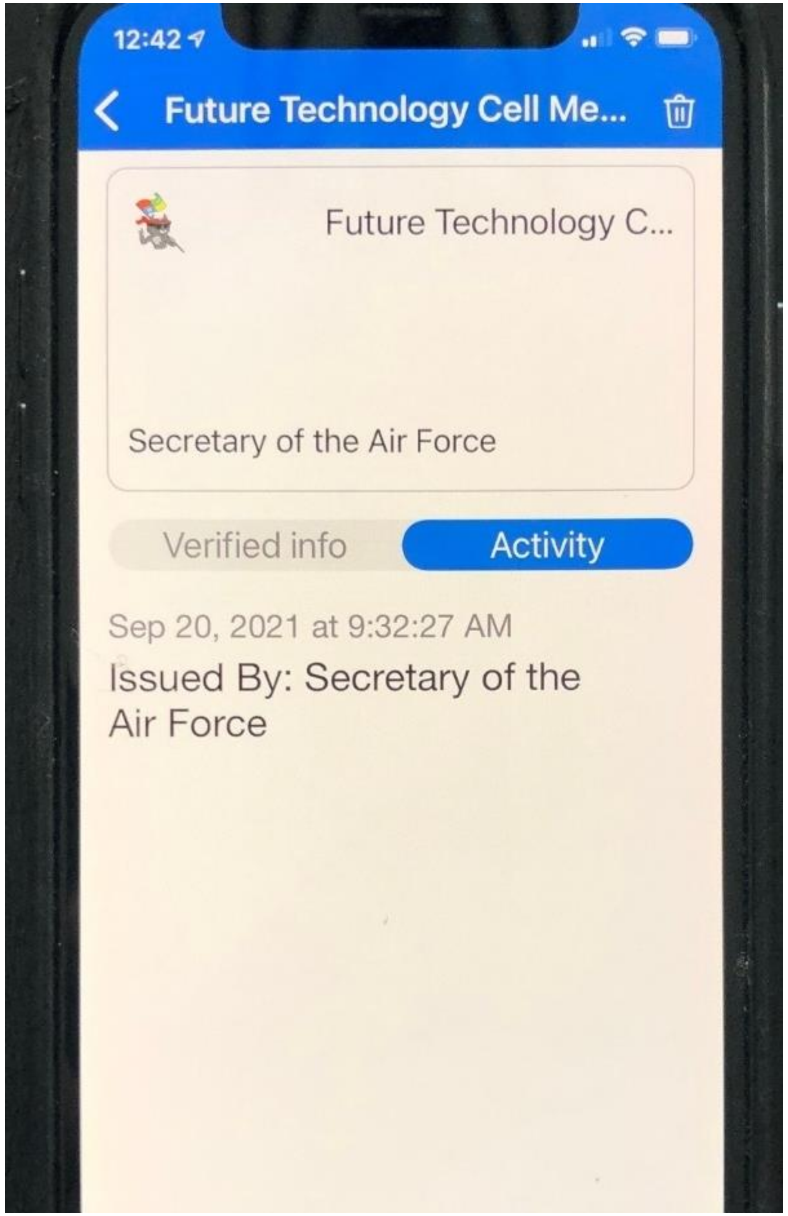
Verified Credential Expert

Verified Credential Ex...

Microsoft

Oct 27, 2021 at 12:59:35 PM
Presented to: Sample Verifier

Oct 27, 2021 at 12:54:41 PM
Issued By: Microsoft



Future Technology Cell Me...

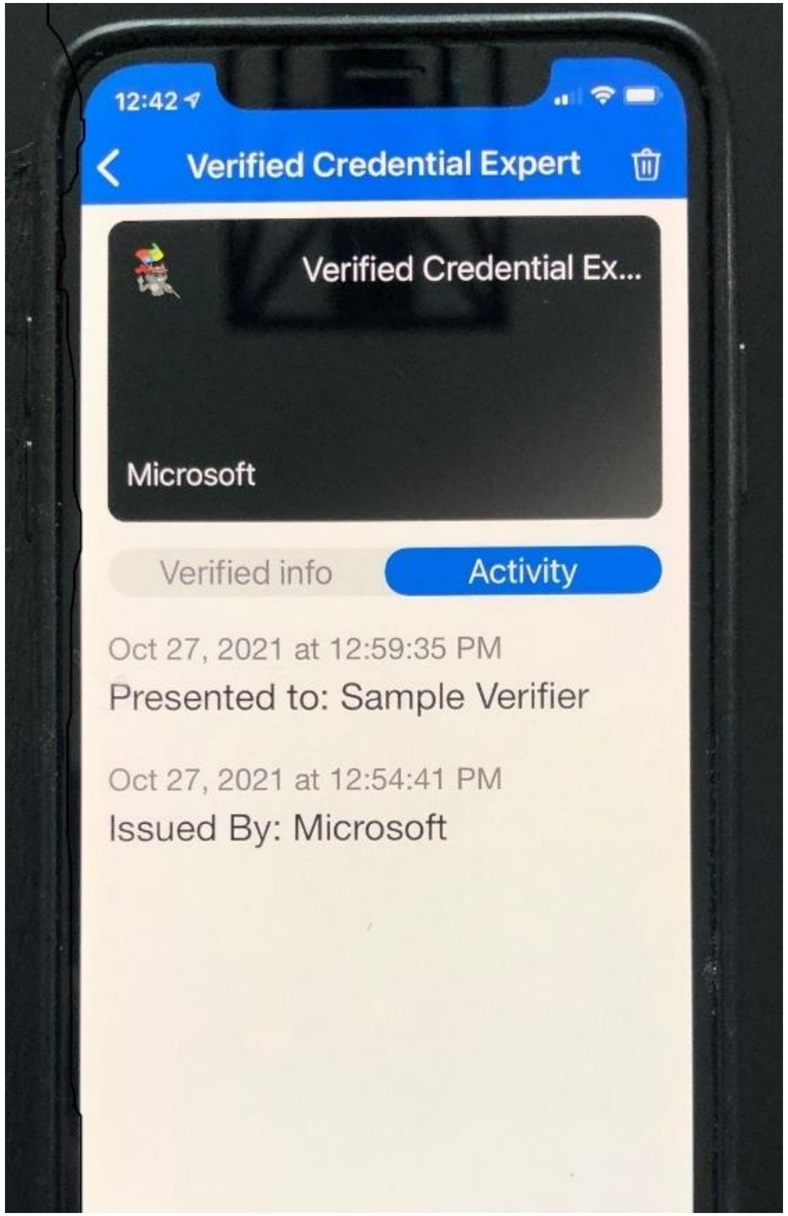
Future Technology C...

Secretary of the Air Force

Sep 20, 2021 at 9:32:27 AM
Issued By: Secretary of the Air Force

IOS EXPERIENCE

IOS EXPERIENCE



Verified Credential Ex...

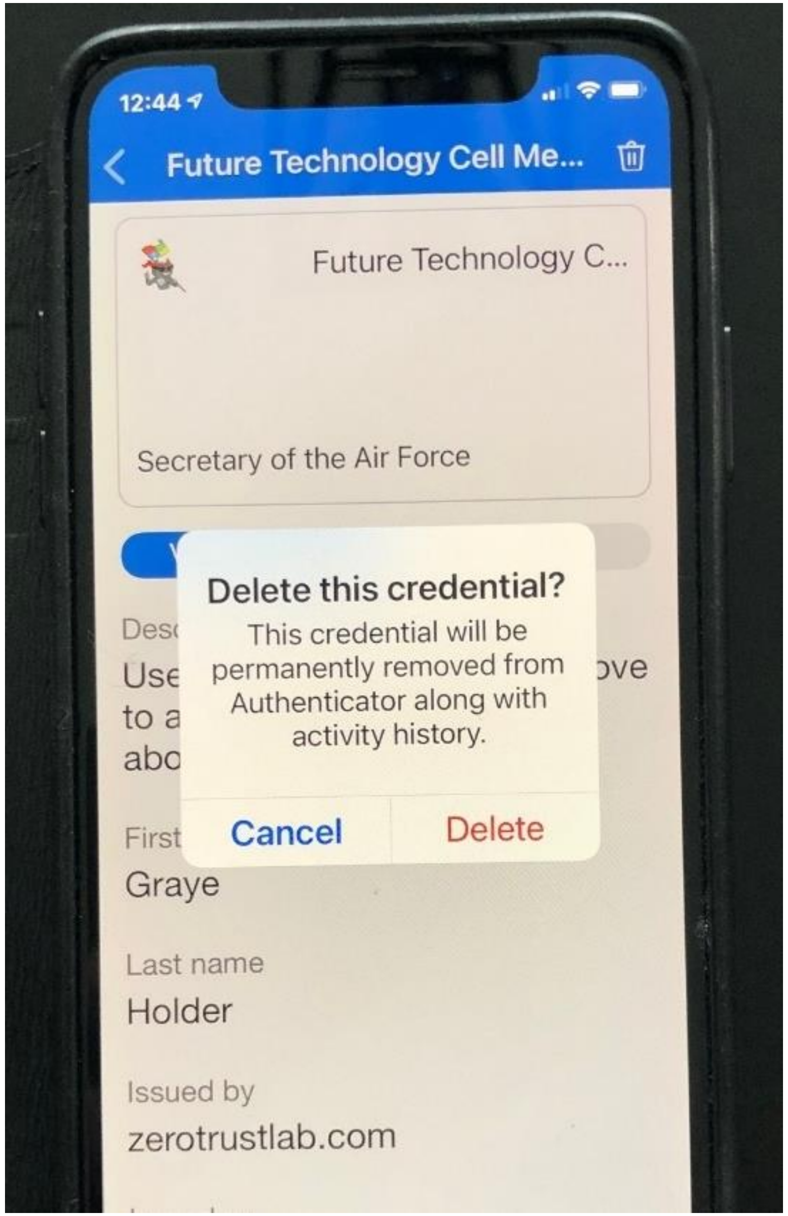
Microsoft

Oct 27, 2021 at 12:59:35 PM

Presented to: Sample Verifier

Oct 27, 2021 at 12:54:41 PM

Issued By: Microsoft



Future Technology C...

Secretary of the Air Force

Desc

Use ove

to a

abo

Delete this credential?

This credential will be permanently removed from Authenticator along with activity history.

First

Graye

Last name

Holder

Issued by

zerotrustlab.com

OBJECTIVE

- The objective of this session is for attendees to comprehend W3C Verifiable Credentials

SAMPLES OF BEHAVIOR

- Define the W3C Verifiable Credential
- Identify the properties of a Verifiable Credential
- Compare and Contrast Verifiable Credentials to other Credentials
- Explain how Verifiable Credentials may impact USAF ICAM Programs and Systems
- Draw a basic verifiable credential architecture
- Using a digital wallet show and explain how a verifiable credential is issued, protected, and verified
- Define a Non-Fungible Token (NFT)
- Using a digital wallet show and explain how an NFT is issued, protected and stored
- Value the use and security a Verifiable Credential provides

VERIFIABLE CREDENTIAL APPRENTICE CERTIFICATE – PERFORMANCE REVIEW AND ISSUANCE

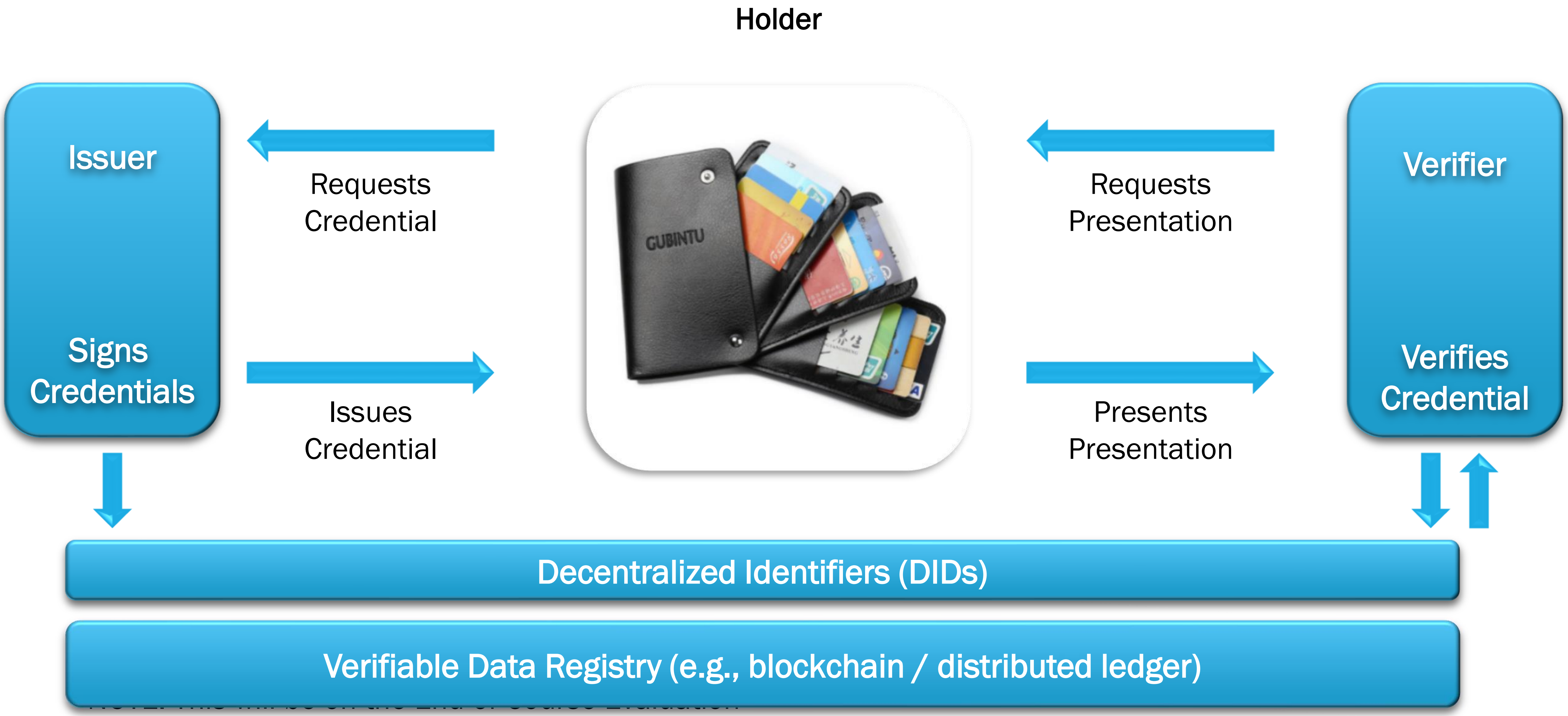
Air Force Form 1256 – Certificate of Training (Apprentice Level)

- Draw a Basic Verifiable Credential Architecture Diagram take picture and send to @Graye Holder in Mattermost and state you have the tools needed installed on a mobile device
  - Microsoft Authenticator – Verifiable Credentials
  - WallaWallet – Hedera TestNet xfer of 1 Hbars from 0.0.15844788 with timestamp and note that account holder has a completed certificate good for 3 years from timestamp
- HCS Topics – Future concept
- Hedera issued NFT when available from WallaWallet – Future concept

Future – ION Network and Hedera Network NFTs (Journeyman Level)

- did
- NFT

BASIC VERIFIABLE CREDENTIAL ARCHITECTURE



Holder

Issuer

Signs Credentials

Requests Credential

Issues Credential

Requests Presentation

Presents Presentation

Verifier

Verifies Credential

Decentralized Identifiers (DIDs)

Verifiable Data Registry (e.g., blockchain / distributed ledger)

WHY DO YOU WANT TO BECOME A VERIFIABLE CREDENTIAL APPRENTICE?

- Driving Forces
- Impress
  - Friends
  - Family
  - Your mother

VERIFIABLE
22 APPRENTICE 01
CREDENITAL

DRIVING FORCES

- Cloud -hosted services
- Smart-Card Limitations
- Zero-Trust
- Technology Tidal Waves

CLOUD-HOSTED SERVICES

Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Network Access

Scalable and Elastic

Shareable

Physical or Virtual Resources

Self-Service Provisioning

Administration on-demand

1 ISO 17788 CLOUD COMPUTING - OVERVIEW AND VOCABULARY

WHAT FUTURE TECHNOLOGY CELL HEARS CUSTOMERS SAY – SMART CARD LIMITATIONS

Do not support the various application [JOSCE] use cases composed of broadly diverse and geographically dispersed population of users [learners]

Solutions that require physical tokens pose significant logistical challenges

Associated costs for implementing most DoD-approved solutions at application [JOSCE] use case scales is prohibitive for a single technology investment

AKA smart-card limitations

ZERO TRUST

- Who
- What
- Where
- Why
- When
- How
- AKA every transaction must be trusted
- AKA nothing can be trusted

NON-FUNGIBLE TOKEN - DEFINITION

- A digital certificate of authenticity used to assign and verify ownership of a unique digital or physical asset; unlike fungible tokens, NFTs are not interchangeable with one another
- Ref: https://unstoppabledomains.com/learn/what-is-an-nft-domain

TECHNOLOGY TIDAL WAVES

- Web 3 – The Token Economy – A total new approach to ICAM
- Zero Trust leads to segmentation
- Distributed Ledgers – Trustless computing
- Decentralized Applications (dApps)
- IoT
- Digital Wallets and Agents
- Decentralized Identifiers
- Verifiable Credentials
- Non-Fungible Tokens (NFTs)
- Verifiable Claims – Why trust when you can prove

CREDENTIAL TECHNOLOGY – 5 YEARS FROM NOW?

- Q: What will it look like, what will it feel like, what security will it bring to the end-user?
- A: It will look like a person carrying a mobile device. The device will have the credentials on the device itself. The security of the credential will be based on the private key protection provided by the device and the issuance and vetting processes of the credential.
- Q: What is a foundational architecture? Big Takeaway Identity Providers (IdP)s don't exist.
- A: The foundational architecture will very much look like real world credential architectures in use for everyday situations (schools, driver's license, and credit cards) some architectures will take advantage of Distributed Ledger Technology (DLT) as their Verifiable Data Registry (account database). The big advantage of using DLT credential holders (people and machines) is that they can be given complete control over private data, Zero Trust.
- Q: If there is no known identity provider, how are credentials revoked?
- A: Credentials can be revoked by an issuer or a holder or both an issuer and holder based on the Decentralized Identifier (did) specification of the credential. It is mandatory for any did to specify how an identifier is created / read / updated / deleted from a verifiable data registry.
- Q: How will credential management change?
- A: Governance, issuance, and validation architectures will change and use digital wallets and agents to handle cloud service interfaces. More dApps and Appnets.
- Q: Can Verifiable Credentials meet NIST 800-63-3 Digital Identity Guidelines?
- A: Yes, for example the Verifiable Credential Apprentice credential is an IAL2 / AAL2 credential, and the Verifiable Credential Journeyman Credential is an IAL 3 / AAL 3 Credential.