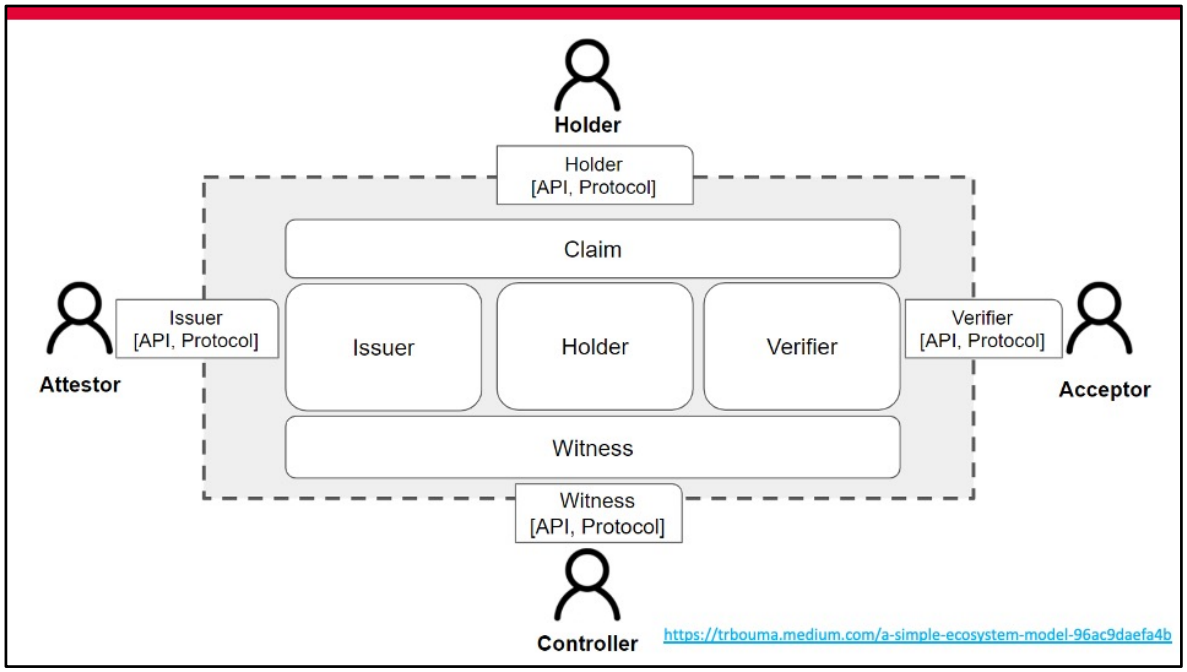
Hello, I'm Andrew Johnston, VP Standards Development and Industry Relations at 2Keys, an Interac Company.

As part of the User Centric Verifiable Digital Credentials Challenge, 2Keys focused on use-cases for foundational identity credentials, and examined four different approaches to interoperability in a digital credential ecosystem.

Today, I'll be illustrating the importance of digital foundational identity credentials to public- and private-sector digital service delivery.

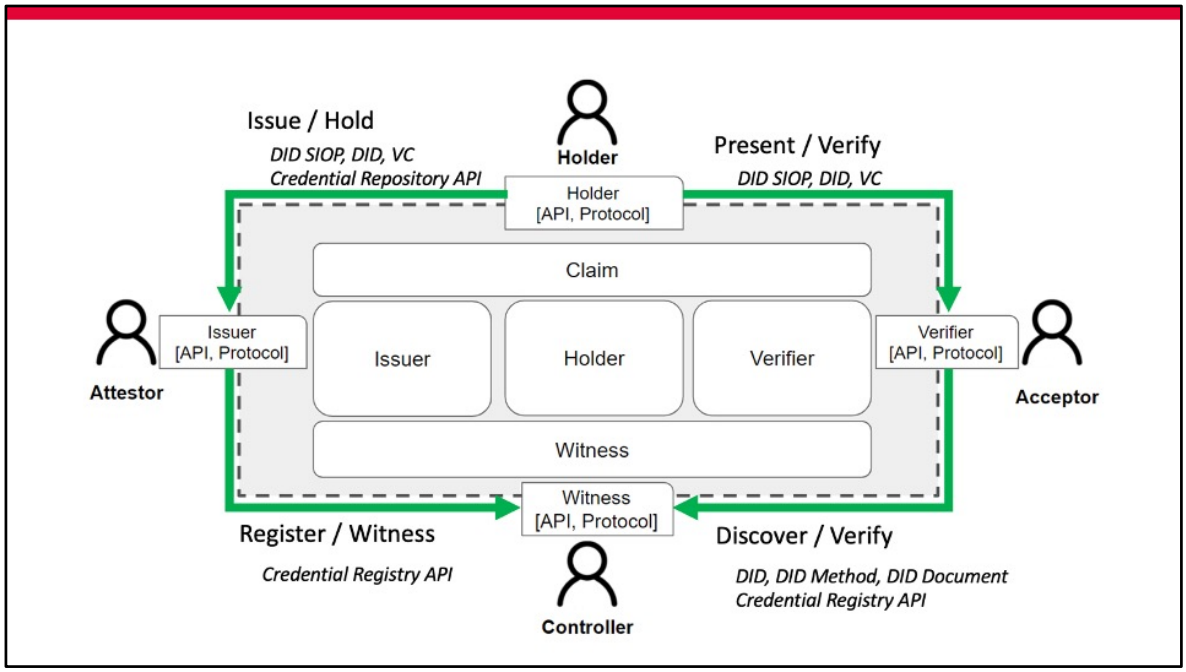
In our first scenario, and the starting point for all the others, a government authority issues a digital birth certificate as a Verifiable Credential to a sample mobile wallet app. Then, the Holder of the newly-issued credential presents it to qualify for an unrelated government service.

Our aim in this is to demonstrate the criticality of digital foundational identity credentials to any online service delivery context, and to show the value of the user-centric credentials approach with foundational identity credentials by decoupling the systems and participants in an ecosystem.



All of the interoperability approaches explored by 2Keys were evaluated in the context of a common ecosystem model with key enabling components of Issuer, Holder, Verifier, and Witness.

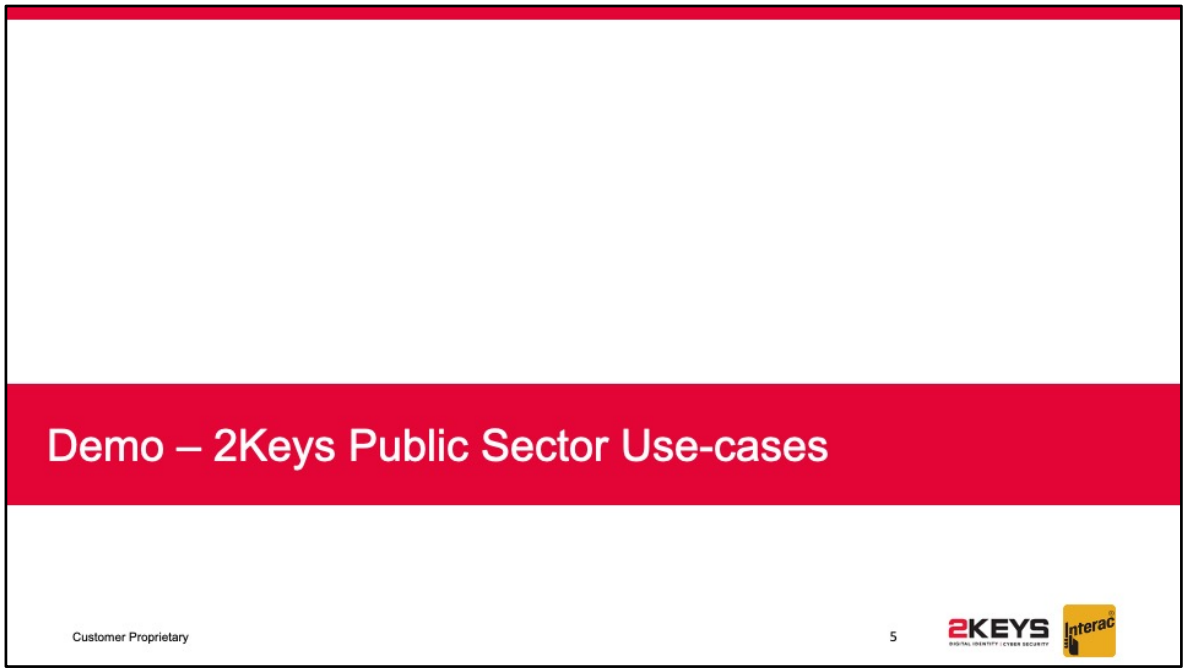
In each case, 2Keys developed the necessary Issuer, Holder, Verifier and Witness components that implemented the specified interfaces.



For this first approach, we rely on established industry standards, like OpenID Connect, and some more recent specifications like W3C Verifiable Credentials, to support interoperability among Issuer, Holder, Verifier and Witness.

2Keys developed some sample applications to demonstrate how each of these approaches might work from an end-user's perspective.

2Keys thinks this approach of relying on standards to enable communication from one component to the next will provide great flexibility, and support the necessary scaling to national, and international, credential ecosystems.



We start our demonstration assuming that the Issuer of foundational identity credentials has appropriately authenticated the person requesting them. Having connected with a Holder app -- see the left side of the screen here -- our Subject may now request a digital birth certificate. Now our Issuer -- the vital statistics authority in this example -- issues a W3C Verifiable Credential by conveying it to the Holder, and registering its existence with a Witness. A representation of the credential appears in the Holder, available for future use.

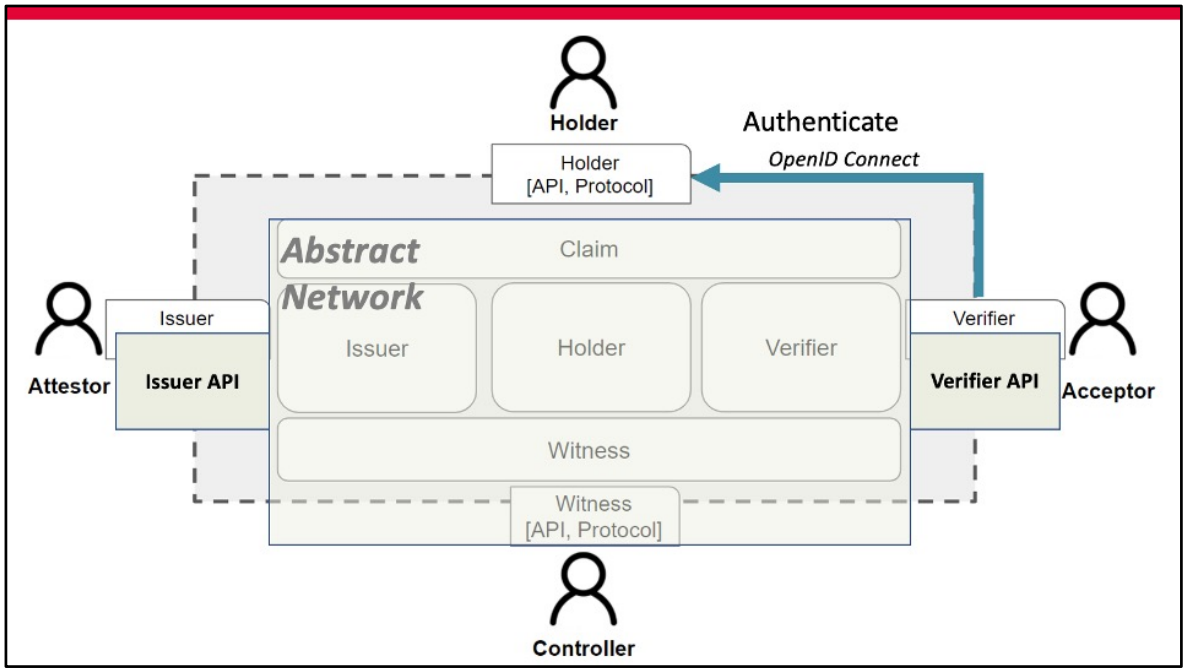
Now our Subject requests service from a different government program. When they choose to use their Digital ID, the Verifier -- the government program -- makes a request for authentication, and for foundational evidence of identity. The Subject reviews this request, and the proposed response based on the digital birth certificate that is in their Holder app. The Subject agrees to present this digital identity credential information to the Verifier.

The Verifier receives the foundational digital identity credential information, and confirms with the Witness that the credential has not been revoked. You'll see now that the Verifier has accepted the identity information, and asks the Subject for some additional program-specific information. Given information that agrees with their

records, plus the verified identity credential information, the Verifier recognizes the Subject as someone already enrolled in the program.

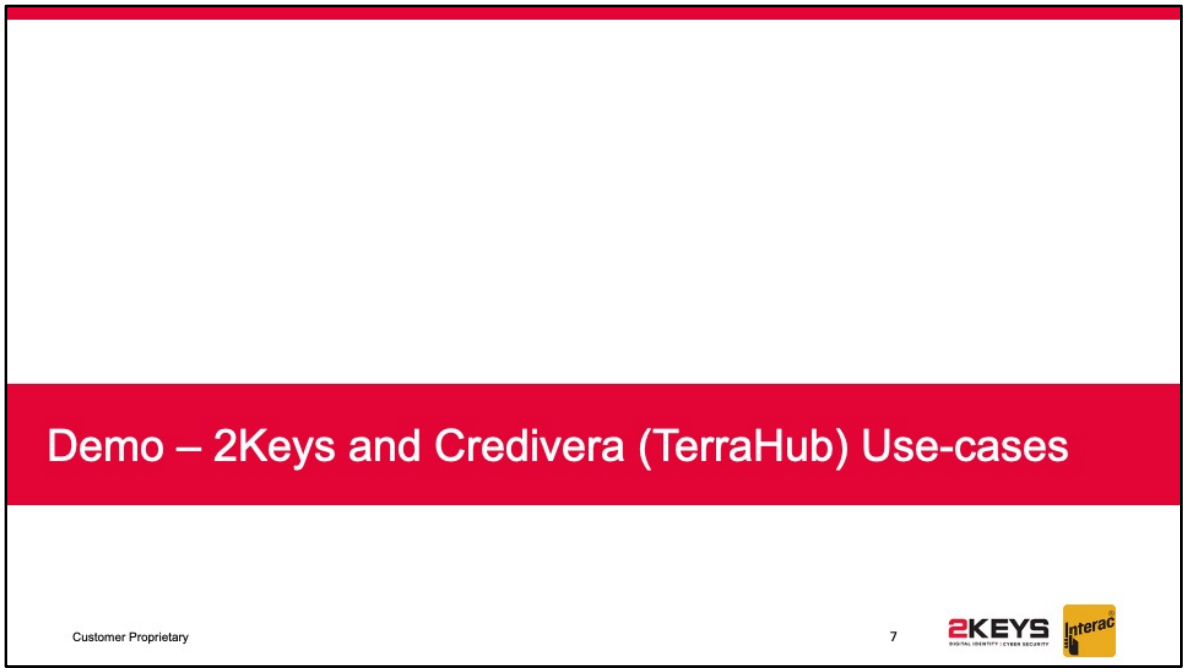
Note that the Issuer and Verifier do not need to integrate with one another to enable this. They both follow the same set of standards, and allow the Subjects to determine if, when, and under what circumstances these credentials may be used. This is the hallmark of user-centric credential systems.

The recognized Subject may now choose to have a digital, program-specific, contextual credential issued to them. Because they have already authenticated with the Holder app, when that W3C Verifiable Credential is issued by the government program, a representation of it appears in the app on the left.



For the second approach to interoperability, 2Keys looked to the work of the W3C Credentials Community Group, and the interoperability efforts supported by the US Department of Homeland Security's Silicon Valley Innovation Program. The minimal API they specified for Verifiers could be combined with OpenID Connect to abstract much of the ecosystem model and greatly simplify integration.

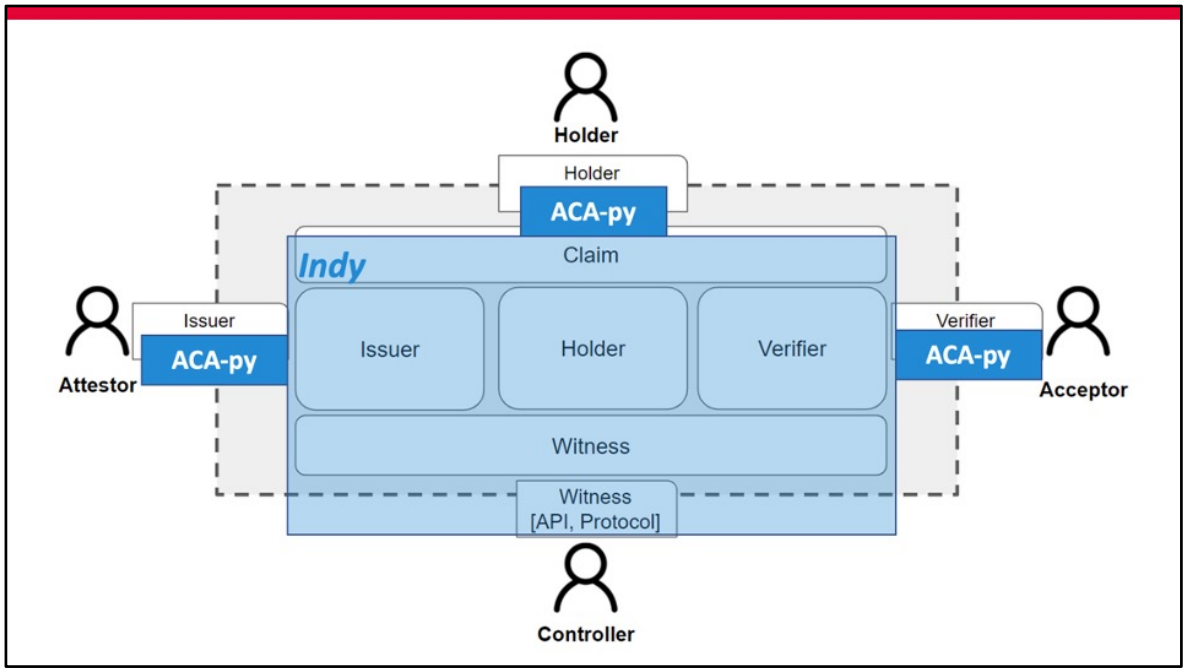
To demonstrate this, 2Keys worked with our friends at TerraHub. They have an application that collects work-related credentials that you'll see more of in their demonstration this afternoon. Here, our Subject with a digital birth certificate uses it to enrol with the TerraHub application -- a demonstration of a potential private-sector use of foundational identity credentials.



As before, the OpenID Connect based authentication triggers a request to our Subject's Holder to present foundational identity credential information. Our Subject approves, allowing that information to be presented to the TerraHub application for enrolment. You can see here that the Subject's name appears on the screen, and a record that represents their foundational identity credentials appears below.

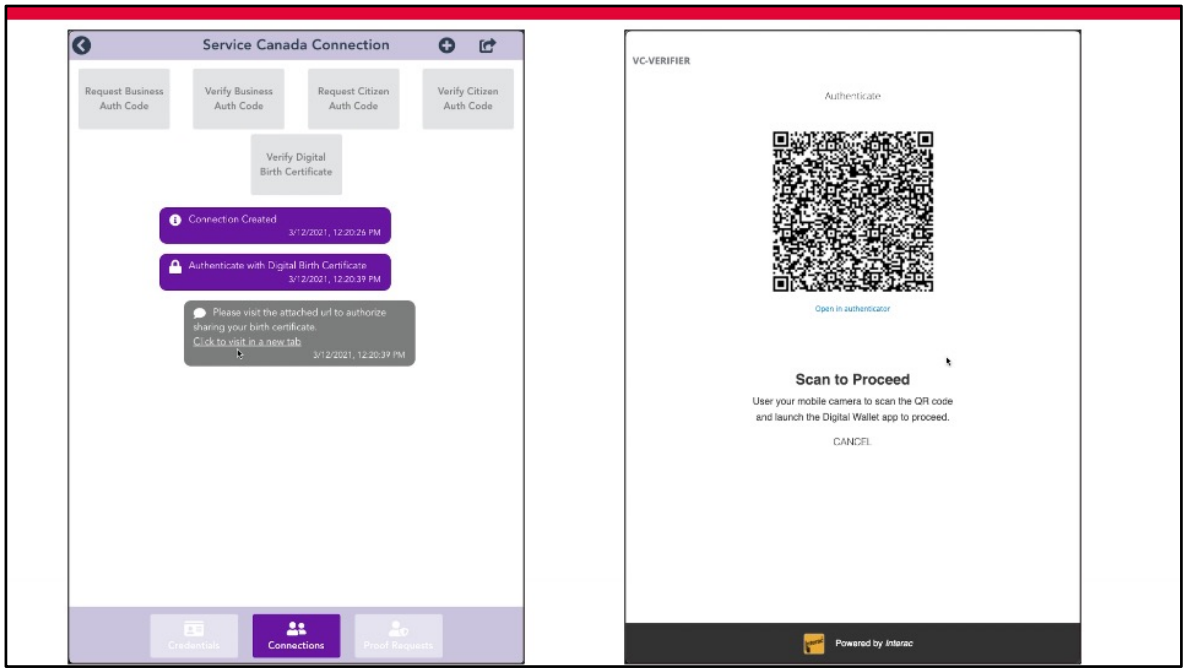
Using the simple Verifier API, the TerraHub application can check to ensure that the status of the credential that was presented has not changed. The application calls the API, and sees that the credential remains in good standing.

Next, we simulate the revocation of the digital birth certificate. The Holder app shows the revised status immediately. When the TerraHub application uses the Verifier API, it can also see that the status of the credential has changed.

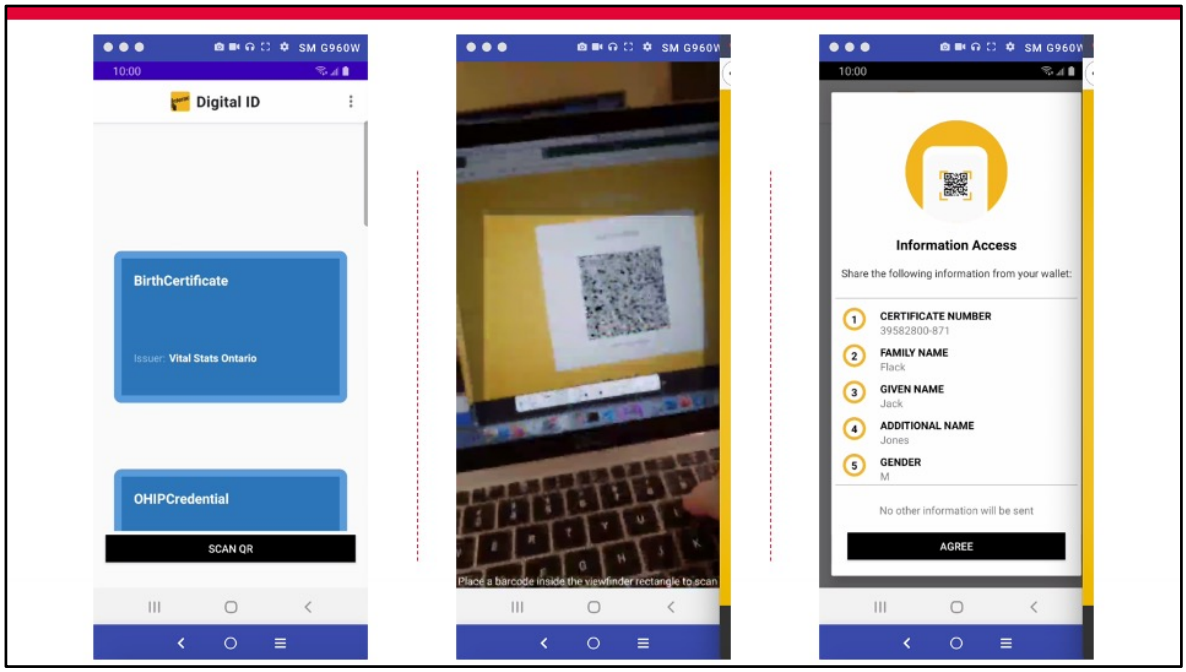


The third approach 2Keys studied with respect to interoperability relies on the integration of applications with a common software stack. In this case, the Witness is provided by a Hyperledger Indy network, and each of the Issuer, Holder, and Verifier used the Hyperledger Aries Cloud Agent for Python, abbreviated here as ACA-py.

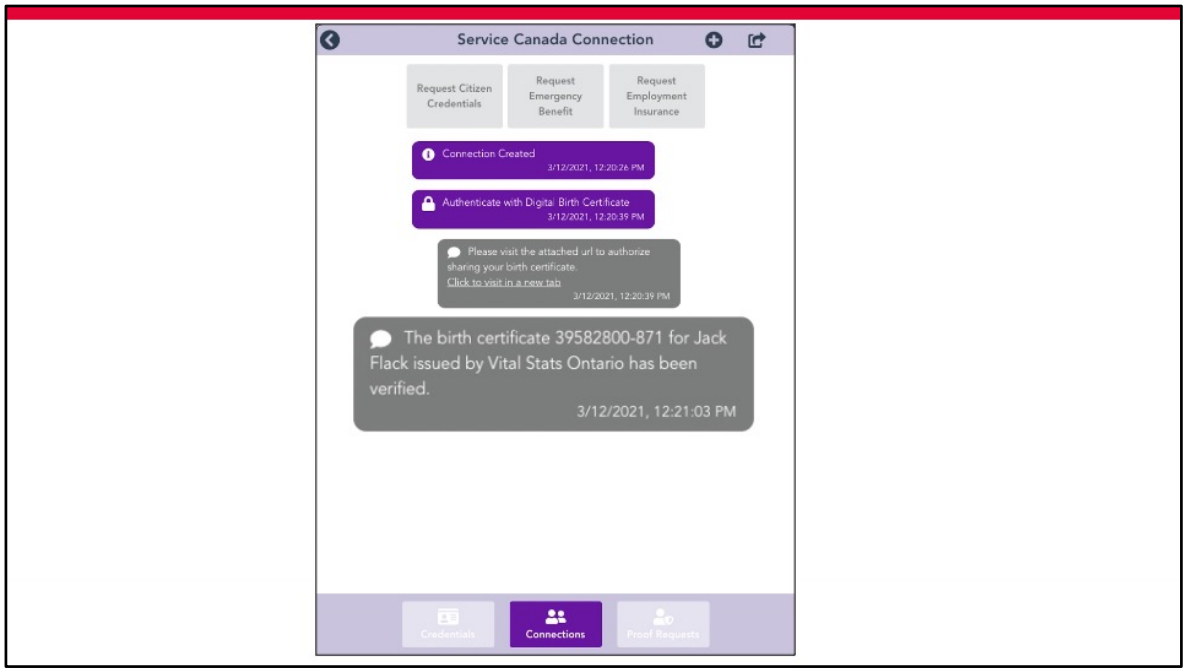
For this approach, 2Keys worked with our friends at Trust Science. In addition to the common software stack approach, the team at Trust Science also showed that they could consume a foundational identity credential from the 2Keys Holder via OpenID Connect.



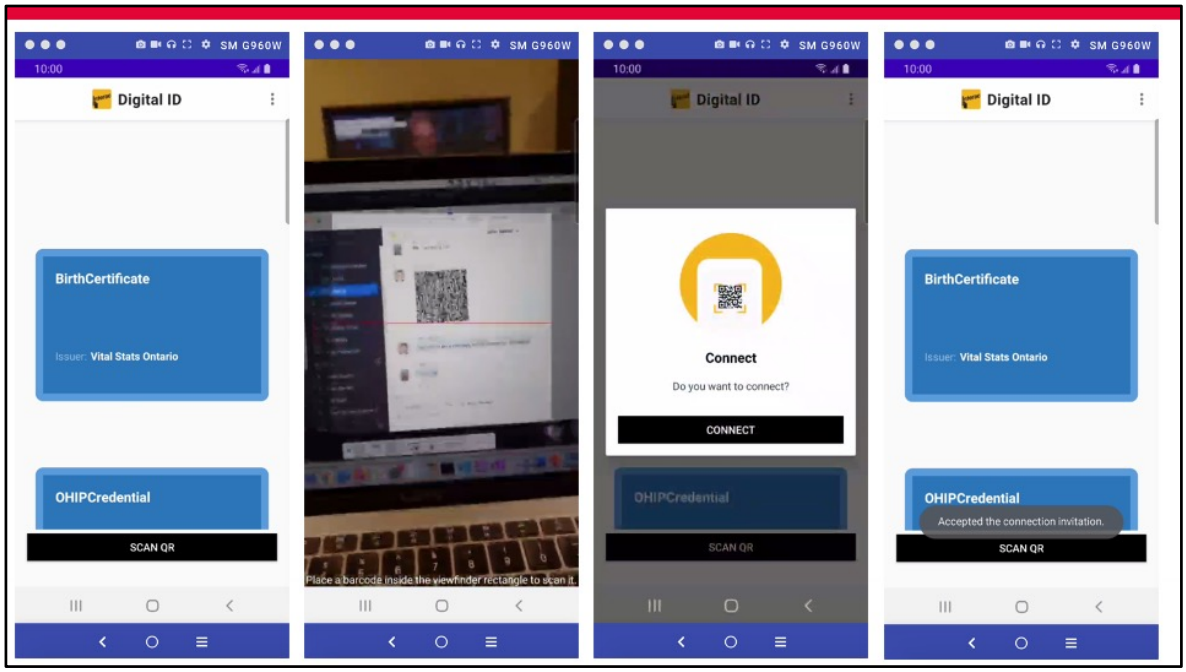
Via the Trust Science chat-like interface, an OpenID Connect authentication follows what is becoming a familiar pattern: …



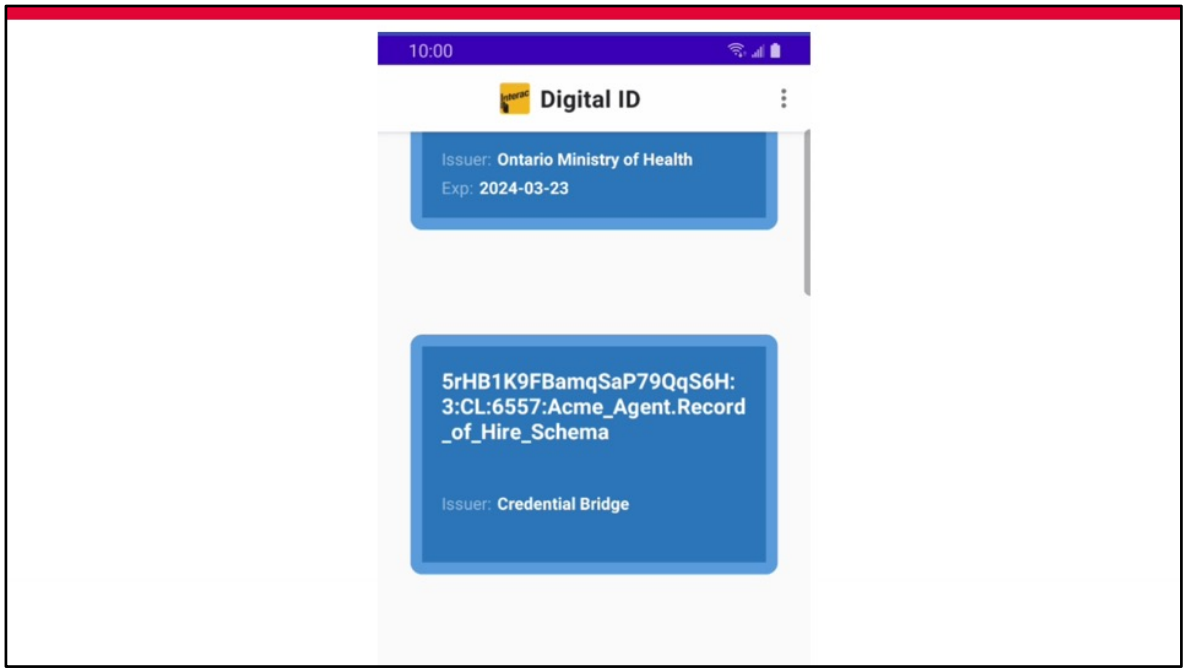
use the Holder app to scan a QR code; authorize the presentation of the foundational identity credential; identity information is presented to the application.



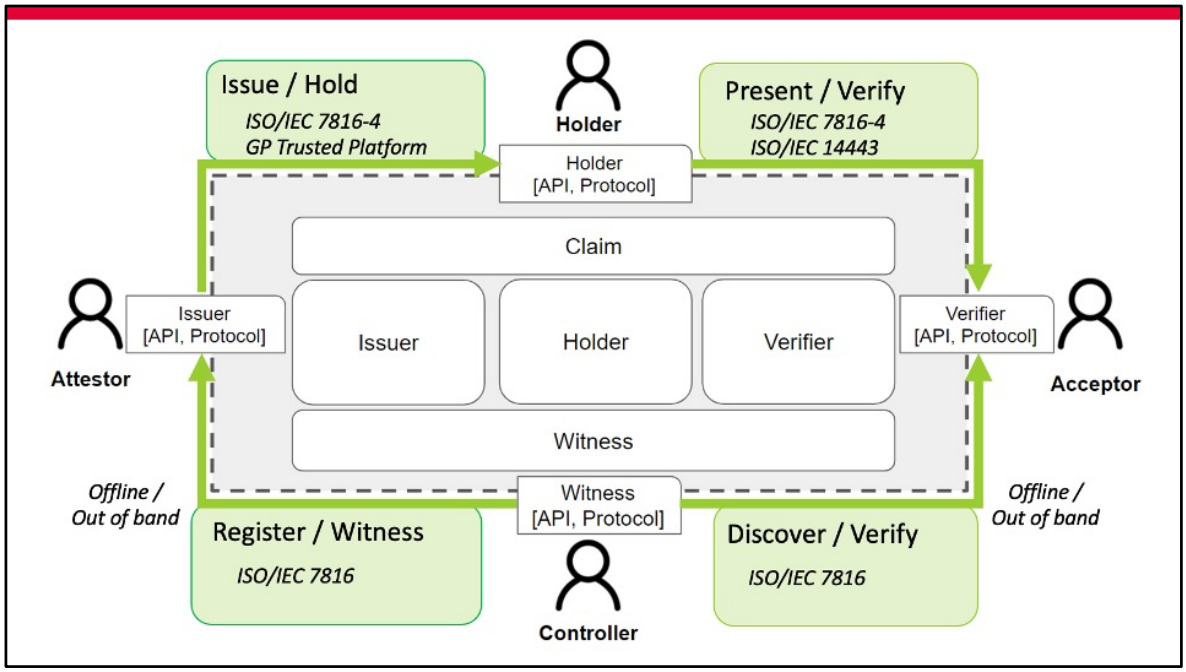
In another private-sector use-case for foundational identity, an employer needs trustworthy identity evidence, illustrated here again with a digital birth certificate.



Demonstrating the third approach, the Trust Science system presents a connection request as a QR code. The 2Keys Holder accepts the connection, and the offer of a Record of Hire credential.

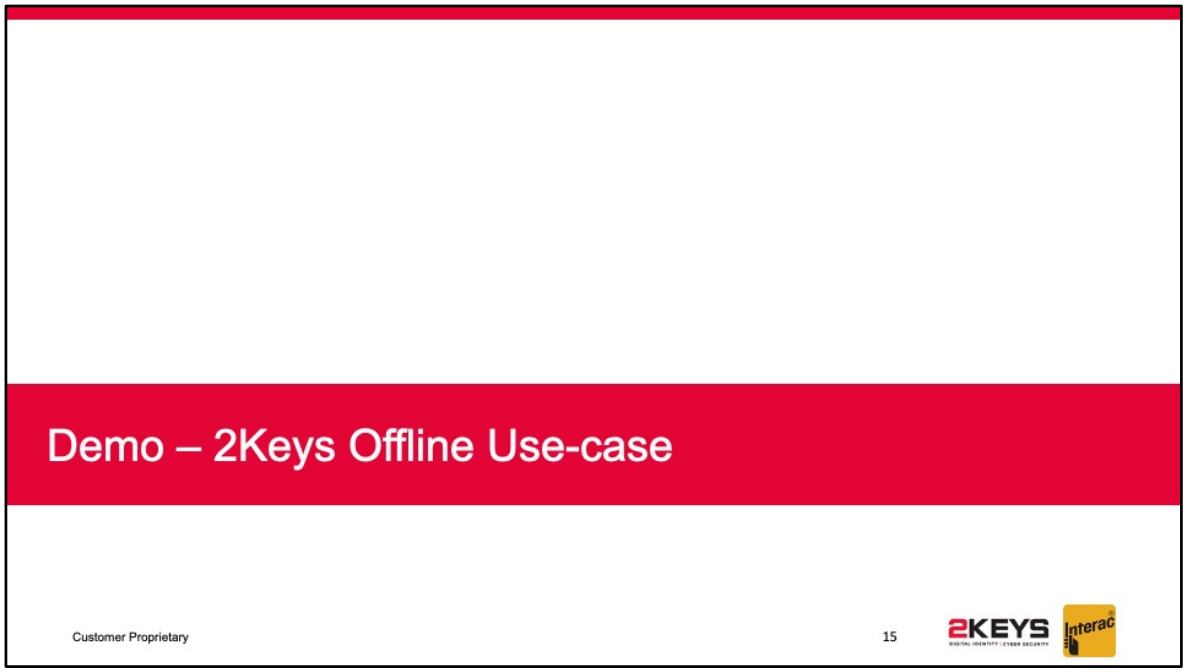


A representation of this credential appears in the Holder app. You'll note here the reference to a credential bridge; this is a component 2Keys needed to develop so the 2Keys Holder could serve as a point of integration.



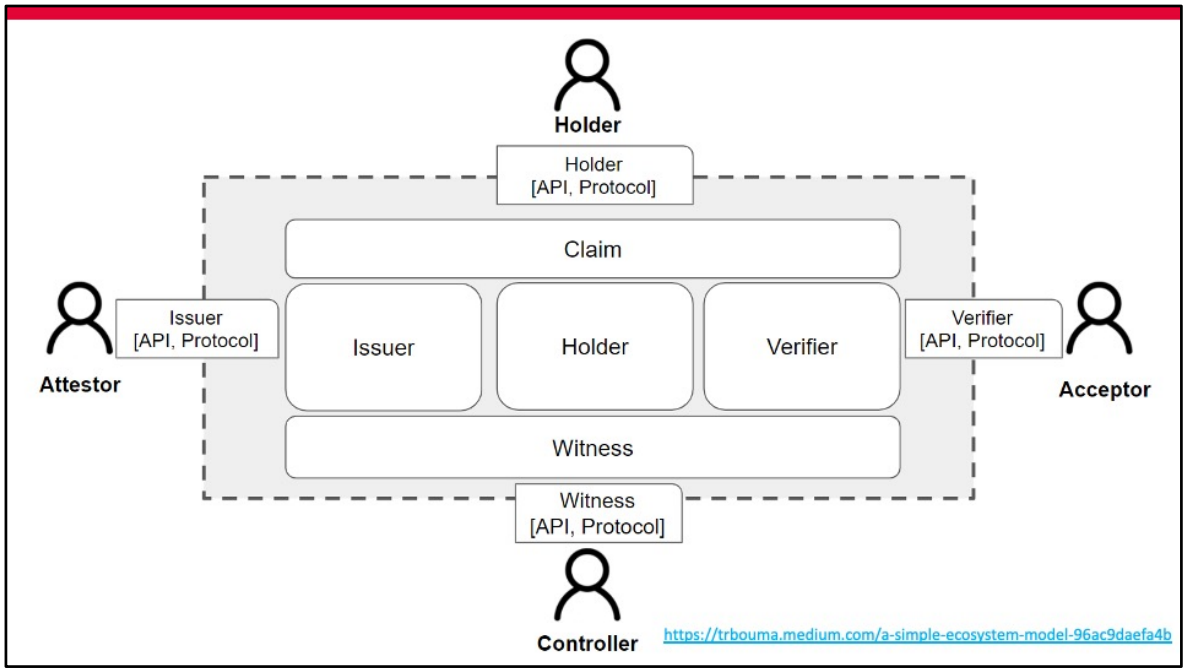
The fourth and final interoperability approach 2Keys investigated supports the presentation of credentials in an offline, or disconnected, environment. Here we rely once again on established, international standards -- in this case, ISO/IEC 7816 part 4, and ISO 14443 to enable the physical presentation of a digital credential via near-field communications, or NFC.

Our use-case here is the presentation of a proof-of-age credential, derived from a foundational identity credential. Let's imagine the sale of age-restricted goods as the driver for proof-of-age evidence. Our Subject is looking to purchase such goods, and the retailer is required to gather evidence our Subject is old enough to complete the purchase. The retailer does not require all the personal information contained in a foundational identity credential, but does require a trustworthy source of proof-of-age evidence.

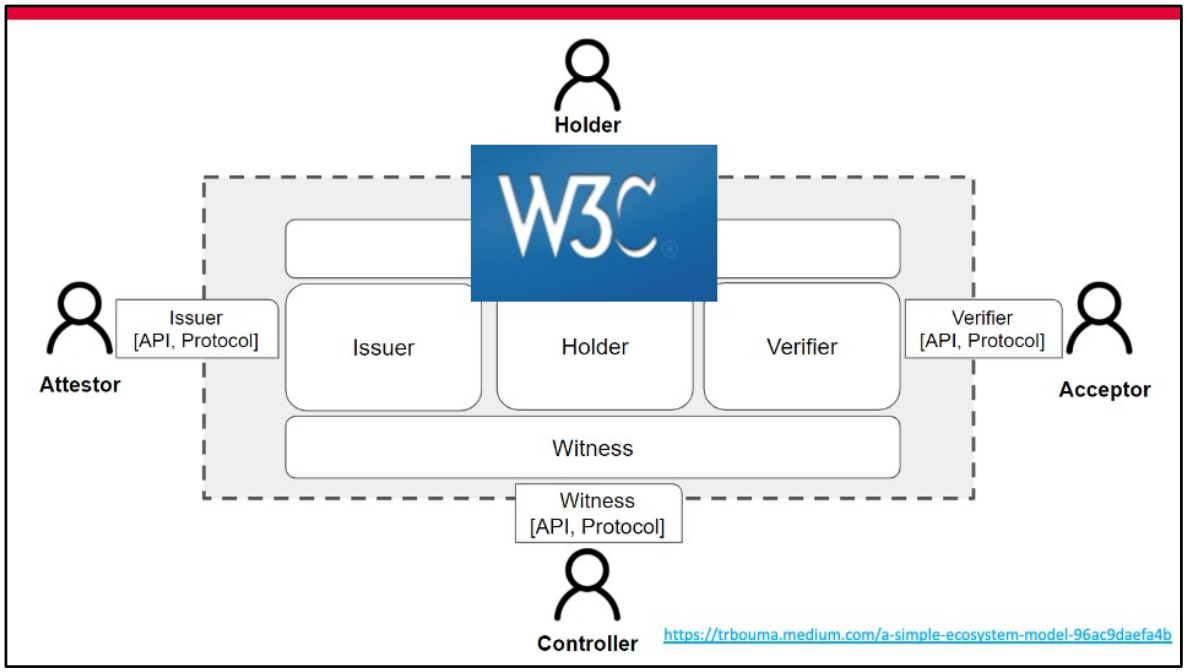


In our demonstration, there are two applications. The first, shown on the left side of the screen, is a Point of Entry or Point of Sale application. This is operated by the retailer in our scenario, to request the presentation of a minimal proof-of-age credential. On the right of the screen is a Holder app running on the mobile of our Subject looking to make a purchase.

When the retailer is ready to accept a proof-of-age credential, they set the Point of Sale app to request proof-of-age via NFC. When the Subject is ready, they launch their Holder, and likewise set it to respond to credential requests via NFC. The Subject brings their mobile, running the Holder app close to the device running the Point of Sale app. NFC communications are established, and the Holder presents a proof-of-age credential, and additional evidence it is reliable and trustworthy. The Point of Sale app verifies that the information it receives is consistent with information it is already configured to trust, and displays a friendly green checkmark to indicate that the credential is valid and acceptable.

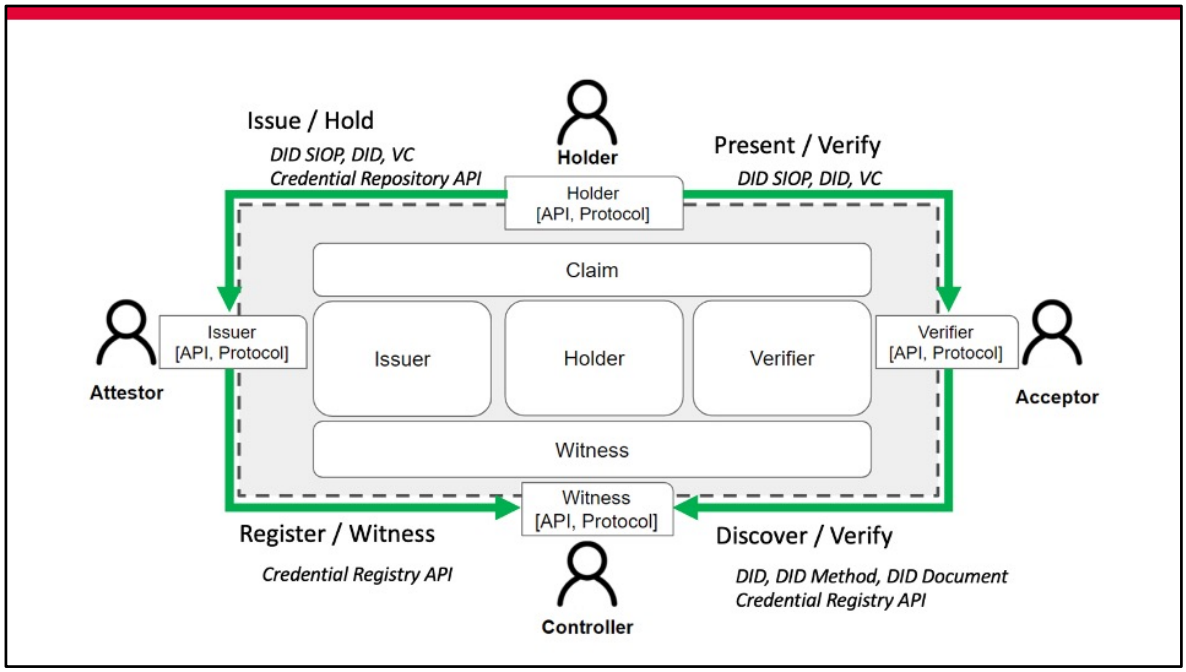


The four approaches to interoperability that 2Keys studied and developed differed in how credentials were communicated among various parts of our model ecosystem.



Another important aspect of interoperability, though, is well-specified representation of claims and credentials. As a cohort, and with the guidance of our Technical Authority, we looked to W3C Verifiable Credentials, and Decentralized Identifiers. With our friends at Bluink, and relying on these evolving specifications, we showed that the 2Keys Holder could accept and independently verify credentials issued by Bluink.

By testing our system against the W3C Credential Community Group's Test Suite, we also developed confidence that 2Keys components could interoperate with solutions from a number of other providers.



While 2Keys examined four differing approaches to interoperability during this challenge, it became apparent that there is a lot of work being done to develop user-centric credential capabilities. Practically, this means that specifications are changing rapidly, and interoperation today is no guarantee of interoperation tomorrow. W3C Verifiable Credentials and Decentralized Identifiers provide a good, general-purpose place to start, but development like the kind we all did during this challenge needs to continue to make them practical for use in the Canadian economy.

Thank You

2Keys Corporation is a subsidiary of Interac Corp.