HYLAND CREDENTIALS

Frequently Asked Questions

1. Are there reasons to use Blockchain as opposed to signed PDFs?

Blockcerts, the open-source standard, provides major benefits that signed PDFs can't:

1. **Independent verification:** Blockcerts can be verified instantly without needing to check with the issuing institution or looking it up in a vendor-owned database. If the school switches vendors or the verification website goes down, people lose the ability to verify PDF documents. With Blockcerts, verification is ensured through a global network that can't be taken down.
2. **Real Ownership:** Blockcerts can be held by students on their mobile device and then shared with anyone they choose for free. They can even share records online, which promotes and highlights the importance of your programs. The Blockcerts mobile app further empowers students by providing a cryptographic connection between the student and their credentials forever, preventing impersonation down the road.
3. **Improved Security:** Blockcerts are tamper-evident and signed by the issuer directly, which can be verified years later without a vendor. Verification includes checking this signature to confirm that a document was really issued by a particular institution on a particular date, thanks to independent timestamping from the blockchain.
4. **Machine Readability:** PDFs are a holdover from the age of paper, and consequently are not easily machine readable. Blockcerts are natively digital, so they are both human readable and machine readable.This allows intake systems to easily make sense of these records upon receipt. This gives your students an advantage when applying for a job or subsequent education.

As your institution prepares for a future where credential exchange is entirely digital, moving to an ecosystem of verifiable, efficient, and secure credentials is a next step you can confidently take.

2. What is the importance of on-chain vs. off-chain data?

On-chain data is stored directly on the blockchain. Off-chain data is stored off of the blockchain (for example, on your hard drive or in the cloud) but can be verified using a blockchain.

A Blockcert is a document (JSON file) that is stored off-chain. It can be verified using a blockchain because its "digital fingerprint" (a hash) is stored on the blockchain. A hash cannot be used to reconstruct the document contents, so the blockchain record can't be "hacked" to reveal document data. This is important for preserving privacy. The Blockcert file can be stored off-chain by saving it or hosting it at a link that can be accessed by

others for easy viewing, sharing, and verification.

Besides a one-way cryptographic hash (digital fingerprint) of the document, the only other data stored on-chain are the public key of the issuer and the date and time of the credential issuance. None of this data can be altered because the blockchain is an immutable record. This makes blockchains useful for decentralized verification by a system, like Blockcerts, which can use the Blockcert JSON file to reference the blockchain transaction via the “transaction receipt” embedded in the file.

3. Can private data be deleted forever?

Yes. If a recipient or issuer wants to delete the off-chain Blockcert, they can simply delete the file. If the file was hosted, they can also take down the link. It is impossible to recover the certificate or any data from the blockchain. The Blockcert references the blockchain, but the blockchain does not reference the Blockcert.

4. How do you verify the identity of a Blockcert issuer?

There are three ways to verify the identity of a Blockcert issuer:

1. Check their public key.

The issuer’s public key is stored both on chain and in the Blockcert file. It is in the interest of the issuing institution to publicize their public key so everyone can know what records legitimately were issued by them. This is why Hyland Credentials builds public key registries for our customers--registries allow you to easily verify that, for example, this is the University of X’s public key and no one else’s.

2. Check their digital signature.

In addition to checking an issuer’s public key, the Blockcerts Universal Verifier always checks the issuer signature on a credential to make sure that the private key used by the issuing institution’s to digitally sign the credential corresponds to the public key in the credential and on the chain. There is a unique cryptographic relationship between public and private key which identifies the issuer and makes sure no one is forging credentials with someone else’s public key.

3. Check the domain hosting the certificate.

Finally, institutions may host the Blockcerts they have issued on their own domains. A verifier can immediately see whether the Blockcert is hosted at the issuing institution’s official domain or on some other domain.

Note that issuers can include images of written issuer signatures in a Blockcert to preserve the traditional look and feel of a paper certificate. Blockcerts are JSON files, meaning they store all the image data, including signature image data, inside. However, Blockcerts issuer identity verification doesn’t rely on a written signature, since that can be easily forged. Instead, issuer identity verification happens cryptographically, through verifying the “digital signature”: the public/private keypair unique to the issuer that was used to sign the credential.

5. How does the Blockcerts Wallet app work?

The Blockcerts Wallet app works just like a private folder. It's stored on a smartphone and cryptographically secured, so nobody but the recipient has access to it. It talks to the organizations that issue credentials so they know where to send them. It also lets recipients keep credentials from many different organizations all in one place on their own devices, so they don't have to rely on anyone else (like a software vendor) to store their credentials. It's not tied to any public identity (like a social media profile or a school account), so recipients choose when and how they want to share the information in their app.

What this means, though, is that the recipient is completely responsible for managing their app. It generates a secure passphrase to which nobody but the recipient has access. Recipients should make sure that they save their unique passphrase in a secure place, like a password manager. This will let them regenerate their app and prove they own their credentials if they ever delete their app or lose their phone. If they lose their passphrase, it's like losing the ID that says you are who you say you are; the recipient will need to contact the issuer to re-issue their credential to them.

6. How do you verify the identity of a Blockcert recipient?

In order to receive a Blockcert, the recipient must be invited by the issuing institution. This access control means that the only people to receive a credential are the people whom the issuing institution has explicitly invited.

The issuer invites a recipient by sending them an email asking them to download the Blockcerts Wallet. The Wallet is a free mobile application available for iOS and Android. The recipient then clicks a button in the email to go to their app store and download the Wallet. Once installed, the Wallet generates a secret private key (unique identifier) for the recipient which, like the issuer's signing key, is never displayed or shared.

There is also a button in the invitation email that the recipient clicks to add the issuing institution to their Wallet as an issuer. When the recipient clicks the button, the Blockcerts Wallet is activated and generates a unique identifier (public key) for the recipient. The public key has a mathematical relationship with the private key in the Wallet that can later be used to verify the recipient's ownership of their Blockcerts.

When the public key is generated, the Wallet sends that key to the issuer. This process is known as "key exchange," and it establishes a secure relationship between issuer and recipient. For security reasons, the issuer cannot issue the recipient a Blockcert until this unique identifier is received.

The Wallet will generate a unique recipient public key for every issuer they add to the Wallet. This prevents data correlation across keys. The recipient can choose whether or not to publicize their public keys, linking them to their known identity. (Either way, public keys cannot be used to access any private documents or data.)

A verifier may issue a challenge to the recipient via the Wallet, prompting them to countersign their Blockcert with their private key. If the private key in the Wallet matches the public key in the Blockcert, the recipient's ownership of the certificate is verified.

7. Can Hyland Credentials access user data, since it flows in and out of the service layer you

provide?

Hyland Credentials is a software application institutions can use to issue Blockcerts at scale. Institutions use the solution to import student data to their account either via CSV or JSON (via API). Under GDPR, this makes Hyland a Data Processor. Like any Software as a Service (SaaS) company, Hyland has data privacy protections in place to safeguard customers' data. This data can also be permanently deleted either after a specified time period or upon request.

8. If, unfortunately, Hyland doesn't exist anymore, how do learners and issuers access their Blockcerts?

Every Blockcert is issued as a digital document (JSON file) and sent directly to the recipient. Issuers also keep a copy of every Blockcert they issue. The Blockcert document references the blockchain transaction which anchored its fingerprint to the blockchain. The Blockcert file can be stored anywhere the issuer and recipient choose, even printed out as a PDF with a QR code. The document can be independently verified using the open source Blockcerts Universal Verifier at blockcerts.org even if Hyland or any other software vendor issuing Blockcerts ceases to exist.

9. When a learner shares his or her credential on social media or with an employer, do others need a private key to see it?

No. Issuers can host their issued Blockcerts as a public link. If the recipient chooses to share this link, the person with the link can verify the Blockcert with no additional software needed. If the credential is not hosted, the Blockcert file can be uploaded to blockcerts.org in order to verify and display the entire credential.

10. For users of the Hyland Credentials Issuing System, what does training include?

The first training session is a one-hour workshop to walk you and your team — as many people as you choose to invite on your end — through every step of the account setup process. A Hyland Services specialist will guide you through the process of test issuing credentials to everyone who provides an email address for the workshop. Subsequent training sessions can also be arranged virtually.

11. Do you do the account configuration or do we do the configuration ourselves?

Hyland configures customer issuing accounts. We will, however, need a liaison in your IT department to work with during the setup process and on occasional account maintenance tasks. You also have the flexibility to configure many of your account settings on your own, should you choose to do so.

12. How long does account configuration usually take?

Initial setup, training, and project planning typically requires one month (30 days) to get to the first issuance of a credential.

13. How many people do we need internally to service our account?

Using your Hyland Credentials Issuing System doesn’t require hiring any new staff. You will, however, need to identify a few account administrators who will help with different aspects of the setup and maintenance process. They are:

Domain Administrator & SMTP Administrator

Often these are the same person, your IT Department lead. They should have access to your institution's DNS service and to your SMTP email settings, so everything can appear that is coming from your organization.

Organization Administrator & Recipient Contact

Oversees account issuing activity. Can also design credentials and manage recipient data. Determines who has access to the system and what permissions they have. This can also be the person recipients reach out to if they have questions or run into any issues. You may also choose to separate these roles.

Communications Lead

This person will work with us to raise awareness about Blockcerts with your student body and internal and external stakeholders. Will will work with them to design email campaigns, website content, FAQ's, videos, and other materials.

14. Do we need specialized people to use Hyland Credentials?

No. The Hyland Credentials Issuing System is a web-based application and can be used by anyone with basic administrative skills. Anyone with a smartphone can receive Blockcerts through the free Blockcerts Wallet (available for both iOS and Android). Verifiers of credentials just need to click a link to access the Blockcert through any web browser. To verify the Blockcert, they can click the "Verify" button on the hosted credential, scan a QR code, or upload the Blockcert file to the Universal Verifier at Blockcerts.org. Verification is instant and free.

15. Do we need to know how to program Blockchain to use Blockcerts?

Not at all! You don't need to buy any tokens, run a node, join a consortium, or even know what the blockchain is to immediately see the value of verifiable credentials. It's super easy to use for issuers, recipients, and verifiers.

16. How long does issuing a credential take?

Issuing a credential to a blockchain can be very fast or take time depending on the institution’s process and workflows. Within the Hyland Credentials Issuing System, the issuing process involves the following steps:

1. Design your certificate
2. Import your recipient data and map it to the certificate

3. Review and approve the certificate template
4. Review and approve the certificate data
5. Schedule a date and time for certificate issuance
6. Issue the certificate

Once issuing is initiated, the amount of time it takes to write the credentials to the blockchain depends on the block confirmation times and network traffic of the blockchain being used. Network traffic and block confirmation times are different for different blockchains (Bitcoin, Ethereum, Hyperledger, etc.), but virtually all transactions are processed within a half hour. Once the credentials are written to the chain, they are automatically emailed to the list of recipients the issuer has designated.