

Secure Digital Vaults for Communicating Shareholder Identities Securely

This document contains proprietary information of Instant Actions

and may not be reproduced, disclosed, or used in whole or in part without the express written permission of Instant Actions. © 2020 Instant Actions

Secure Digital Vaults for Communicating Shareholder Identities Securely

Background

Data effectively has two states – ‘at rest’ and ‘in transit’. For data to remain secure and for the owners and controllers of data to be seen to be exerting all reasonable efforts to keep that data secure, it is important that care and consideration is given to how data is treated in both of those states.

When data is static within a database or a file server, it is said to be at rest. In the context of SRD2, it could be thought of being at rest as it sits in the intermediary’s database waiting to be extracted by the intermediary, before being packaged up in to a disclosure for the issuer and delivered via a number of different means. Once received by the issuer, it will likely be placed on a file server or a database somewhere within the issuer’s firewall, once again, being considered to be at rest. Of course, data is always subject to intrusion attacks etc. but when tucked away behind either firm’s firewalls, it can be thought of as being relatively safe. It should be noted that accountability for the safety of the data is also quite easy to determine as should it become vulnerable to bad actors whilst at rest, this will generally be because either the sender or the recipient has failed in some way in respect of their data safekeeping responsibilities. Reasons for this might be that perhaps, despite their security safeguards, a virus or malware has been installed on a device within the firewall or as a result of social engineering, they may have unwittingly enabled a ‘man-in-the-middle’ attack on their systems. Either way, it is generally clear where responsibility and accountability lies – namely with the entity that has failed to take the necessary steps to keep that data safe at rest.

This all changes when the data is in transit and arguably at its most vulnerable. Almost all email (the most prevalent transit mechanism) is sent in unencrypted form and the content is said to be ‘in clear’, in other words, can be read by anyone that wishes to do so. Clearly, in the context of SRD2, this would constitute a critical security failing.



So the key mitigation in keeping data secure when in transit is to limit or ideally eradicate any steps that involve introducing anything less than highly secure, robust measures for handling the data, whether at rest or in transit.

That is precisely what the Instant Actions solution does. It provides the best of both worlds.

Secure Digital Vaults - what are they?

A Secure Digital Vault (SDV) is a secure place used to store important data, for access exclusively by authorised users only. Strict safeguards control who can access the data how the data is encrypted and stored. It should provide comprehensive audit trails to show when and by whom data has been accessed.

Why are they important – what purpose do they serve?

SDVs are important because they provide a controlled environment for sensitive data that should not get into the public domain, but which needs to be accessed by parties who have a legitimate need to access it.

An SDV is a digital space in which the entire content is encrypted with a key held ONLY by the owner. Usefully, however, such vaults can be made accessible online to trusted partners, within a cloud architecture, either selectively or in total.

Instant Actions uses the only currently commercially available SDV with optimised Cloud Architecture and flexible access control optimised for use on a secure communication channel to provide shareholder identity data at the request of an issuer.

The importance of such Vaults is that they provide a way to share information safely, securely and privately. When one party deposits a document or message in a folder within the Vault, the other party's software (which also has access to the relevant part of the vault) will alert its user to the existence of the message. Outside those two parties, not even the Cloud owner will be aware that such a data transfer has occurred. They can be configured to notify trusted counter parties that an encrypted message is waiting, available to download and so act as a secure method of communication. If both counterparties have trusted access to the SDV then you have perhaps the securest 2-way communication channel possible because there are no other parties involved.

How can I use an SDV as a secure channel for transmitting shareholder identities?

The use of an SDV secured in the cloud as a means to communicate data safely is actually very simple. If you use Instant Actions, for your convenience, we orchestrate the creation of your private account, including advice on creating the strong password which (apart from physical access controls) will be the only protection for the data you need. But neither we nor anyone else can ever access your data and the vault belongs to you. You are still the controller of the data and in compliance with GDPR see [\(EU\) 2016/679](#).

Through the use of secure vaults, Instant Actions enables the intermediary to place the sensitive disclosure in a location that is only accessible to the issuer as they will be the only party that has the appropriate vault credentials.

When you receive a disclosure request, IA responds to the reply address on your behalf and the issuer receives a message informing them that the data should be provided to them shortly by means of a SDV. Instant Actions will have vetted the identity of the issuer to an acceptable pre-arranged score based on criteria that we have agreed with the intermediary, so they can be satisfied that they are responding to a legitimate original source.

Once they have been given access, data can be exported directly and safely by the issuer to a local location within their firewall. Upon having been downloaded, the disclosure data is no longer required in the vault and is safely deleted, leaving no trail of sensitive data behind. At that point, that deposited instance of the data (the one that has now been saved to a location within the issuer's firewall) ceases being the intermediary's responsibility and becomes the issuer's responsibility.

Please note that at no time is any sensitive data transferred by insecure means such as email.

Operational Sequence for Validating Issuer Source Identity and using the SDV to Send Shareholder Identities

- 1 Intermediary appoints Instant Actions to seek issuer identity validation on their behalf.
- 2 Instant Actions (IA) validates the identity of issuers using standard rules set up within the Codel Notary ID enrolment software. See summary of Codel Notary ID software [here](#).
- 3 IA also creates a SDV for the issuer. As described, the SDV is secure and private. The password creation service provides initial credentials delivered manually and digitally witnessed.
- 4 The SDV can be used to prove that the intermediary is controlling the data in compliance with the GDPR directive
- 5 Once the intermediary is formally enrolled, IA sends a message including a one-time link to the reply address contained within the SID request(s). if the intermediary receives the request from more than one source (e.g. different custodians), IA responds to the issuer reply address multiple times depending on how many different intermediaries have received the same request. The reply on behalf of the intermediary says the following;
- 6 Dear Issuer, xyz intermediary ltd have received a request that purports to be from you to send them a list of their shareholders for whom they act. Prior to sending you this data It is an obligation under the terms of SRD2 for them to validate that this request originates from the proper authority and is genuine. They have appointed us to do this for them. You should confirm that we have been properly appointed by checking with them at their company by contacting Luke Skywalker at Star Wars Plc. If you wish to proceed, go to www.instant-actions.com and check that your browser recognises our SSL certificate as genuine. Then look for the button labelled "Identity Enrolment" where we will walk you through an Identity Verification procedure. You will only need to do this once. You may also appoint an agent to act for you by setting up an administrator however the admin will also need to go through similar identity checks. With your (optional) permission, we will keep your information on file or delete it as soon as you have confirmed, your identity and that you are the sources of the SID request. If you opt for your contact data to be deleted you will of course have to enrol the next time you receive a request from an intermediary to validate your identity in response to a SID request. Before responding to this message, if you have not already done so, you should check that www.instant-actions.com is a legitimate domain/service. Once you have completed your identity information and confirmed the content of the SID disclosure request, we will notify the intermediary that it is safe for them to send you the data. We have set up a secure channel for them to do this. You will receive a second link which will grant you access

to the data they upload to another SDV specifically set up for the purpose of communicating potentially sensitive shareholder identity information.

- 7 When the issuer receives notification from us that this data is ready to download, they will only be able to retrieve it once because it will have been deleted as soon as they downloaded it, at which point control of it passes to them and they become a data controller under the terms of the GDPR directive. Consent for storing this data has been set both by the intermediary in compliance with GDPR and under SRD2 at 12 months, the maximum period they should store it for unless they need to retain it for other legitimate purposes. Even though they can only download the data once, IA provides a data retrieval and intermediary contact service which allows them to ask them for it again, but this time direct. For ease, the data is provided as a downloadable .csv file.
- 8 The intermediary receives confirmation when the issuer has downloaded the data at which point, they are prompted to delete the data if it has not already been automatically deleted.
- 9 All such data creation, transactions, storage and related messaging are recorded in a dedicated database whose every entry is protected by the Codel immutable audit trail. Complete Codelmarked audit trails which can be verified through an audit dashboard are available on demand to all interested parties, including 3rd party auditors. This enables the intermediary to demonstrate to the regulator that they have explicitly complied with GDPR regulations. The Codel protection ensures the no record can be changed without immediate detection. It doesn't just protect the integrity of the data but also proves the date and time it was registered and the identities of those involved.

For more information go to enquiries@instant-actions.com

Limitations

This documentation contains information that is confidential and proprietary property and/or trade secrets of Instant Actions and/or its affiliates. This documentation is not to be published, reproduced, copied, disclosed or used without the express written consent of Instant Actions. This document is provided for informational purposes only. The information contained in this document is subject to change without notice and does not constitute any form of warranty, representation, or undertaking. Nothing herein should in any way be deemed to alter the legal rights and obligations contained in agreements between Instant Actions and/or its affiliates and their clients relating to any of the products or services described herein. Nothing herein is intended to constitute legal, tax, accounting or other professional advice. Instant Actions makes no warranties whatsoever, either express or implied, as to merchantability, fitness for a



particular purpose, or any other matter. Without limiting the foregoing, Instant Actions makes no representation or warranty that any data or information supplied to or by it are complete or free from errors, omissions, or defects.