Traceability Driver Service: Security

The Traceability Driver Service uses three layers of protection to secure data. The first layer prevents malicious third parties from intercepting messages by using secure, HTTPS connections. The second layer is a control that protects solution providers from data requests by any party that they have not registered as a trading partner. The final layer is public key encryption, which allows solution providers to verify the identity of the party requesting data based on a digital signature.

# What data is being communicated?

The only data being communicated through the Traceability Driver to other solution providers is event data and master data. None of this data is cached in the Traceability Driver, so there each time that data is requested, the solution provider receiving the request must authenticate and return the data requested. They have complete control over the data.

# What data is stored in the Traceability Driver and where is that stored?

The only data that is stored in the Traceability Driver are the added accounts and their associated trading partners. There are no other accounts added.

# HTTPS

HTTPS prevents third parties from intercepting messages by encrypting all communications. Decrypting messages requires an appropriate certificate that is exceptionally difficult to reproduce.

# Trading Partners

To prevent unallowed access to a user’s data, the Traceability Driver Service requires both parties of a data communication be registered as trading partners for each other. This gives the user complete control over who has access to their data. If someone requests data from you, but you have not registered them as one of your trading partners, the request will be denied.

## Trusted Solution Provider

When adding a Trading Partner, this can be done using the Directory Service. When adding the Trading Partner, you can verify the solution provider that is hosting the Trading Partner. For an additional layer of security, you can choose to only add Trading Partners from solution providers that you trust.

Only Solution Providers registered on the Directory Service can query the Directory Service for available accounts.

To query the Directory Service, you need to actual search it. You cannot just get a full list of everyone on the Directory Service.

Could the directory service be used to mine information?

Whole Chain would not add someone to the directory service unless the service requested it. This is a great MO, because it keeps the business in control of adding them to a directory. You do not want to expose any user data without them taking the action. Is there a legal liability around this? The fact a seafood company is using a solution provider is considered confidential information.

# Signed Requests

Every Trading Partner has a public key that is downloaded from the Directory Service. When a Trading Partner sends a request to an account for data, they sign the request using their private key. Then when the request is received, the signature is validated using the public key of the Trading Partner. This ensures that the request was sent by the Trading Partner.

The signature is included as the Authorization Header on the request including the following information:

{

“AccountPGLN” : “urn:gdst:party:TR28401.0”,

“TradingPartnerPGLN” : “urn:gdst:party:WC100.0”,

“Subject” : “urn:gdst:product:lot:class:WC100.0.0000”,

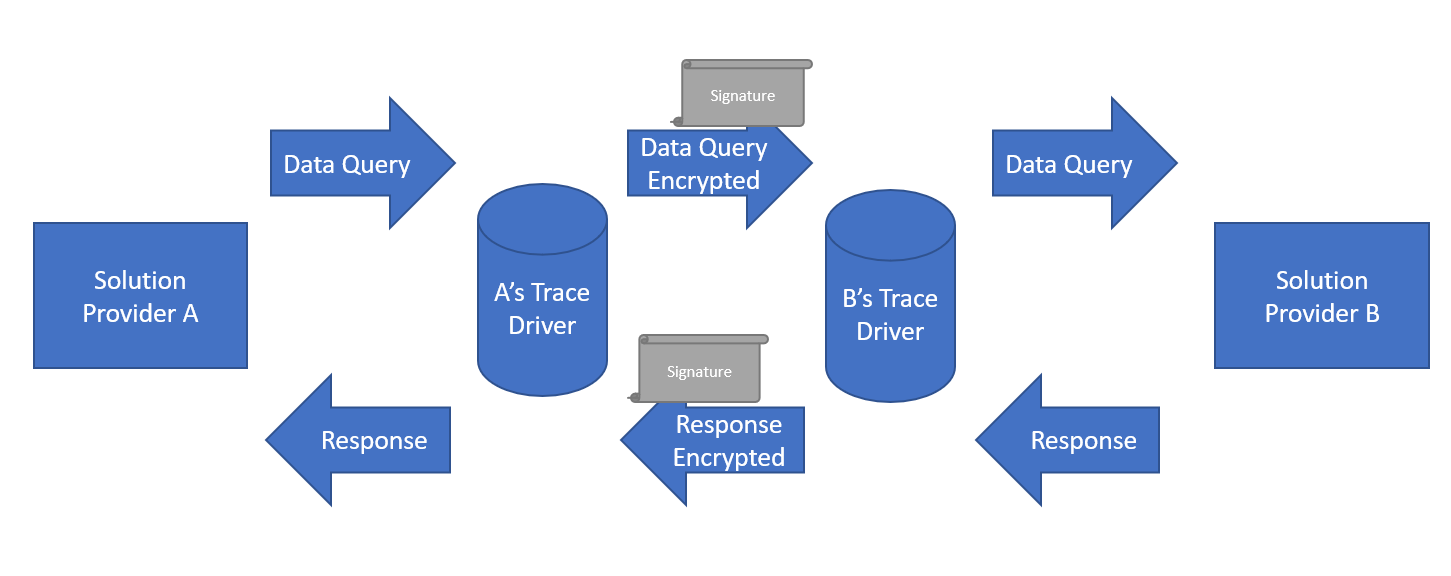
“Nunce” : <UTC Date Time of the Request>,

“Signature” : “ABDHASDSFHSDF813213XUFBADSF..”

}

This signature is encoded into a Base64 string an included in the Authorization Header on every request to ensure that:

1. The Trading Partner created this request.
2. The Account receiving the request was the intended account for the request.
3. The data being request is the intended data to be requested by the trading partner.



# Data Filtering

It is possible to filter the data returned on a trading partner by trading partner basis. This is because when your local API is queried for data, it’s possible to include the following information in each query:

1. What is being queried for? I.E. the GTIN, GLN, PGLN, or EPC
2. Who is the data being queried from? I.E. the account ID.
3. Who is the company asking for the data? I.E. the trading partner ID.

The Account ID tells you which account is being queried, and the Trading Partner ID tells you who is asking for the data. By knowing who is asking for the data, you can use internal logic to return all the data or a subset / filtered version of the data for security purposes.

Could there be a set of guidelines of around what would be common filtering purposes? This could be something that the Consortium could tackle.