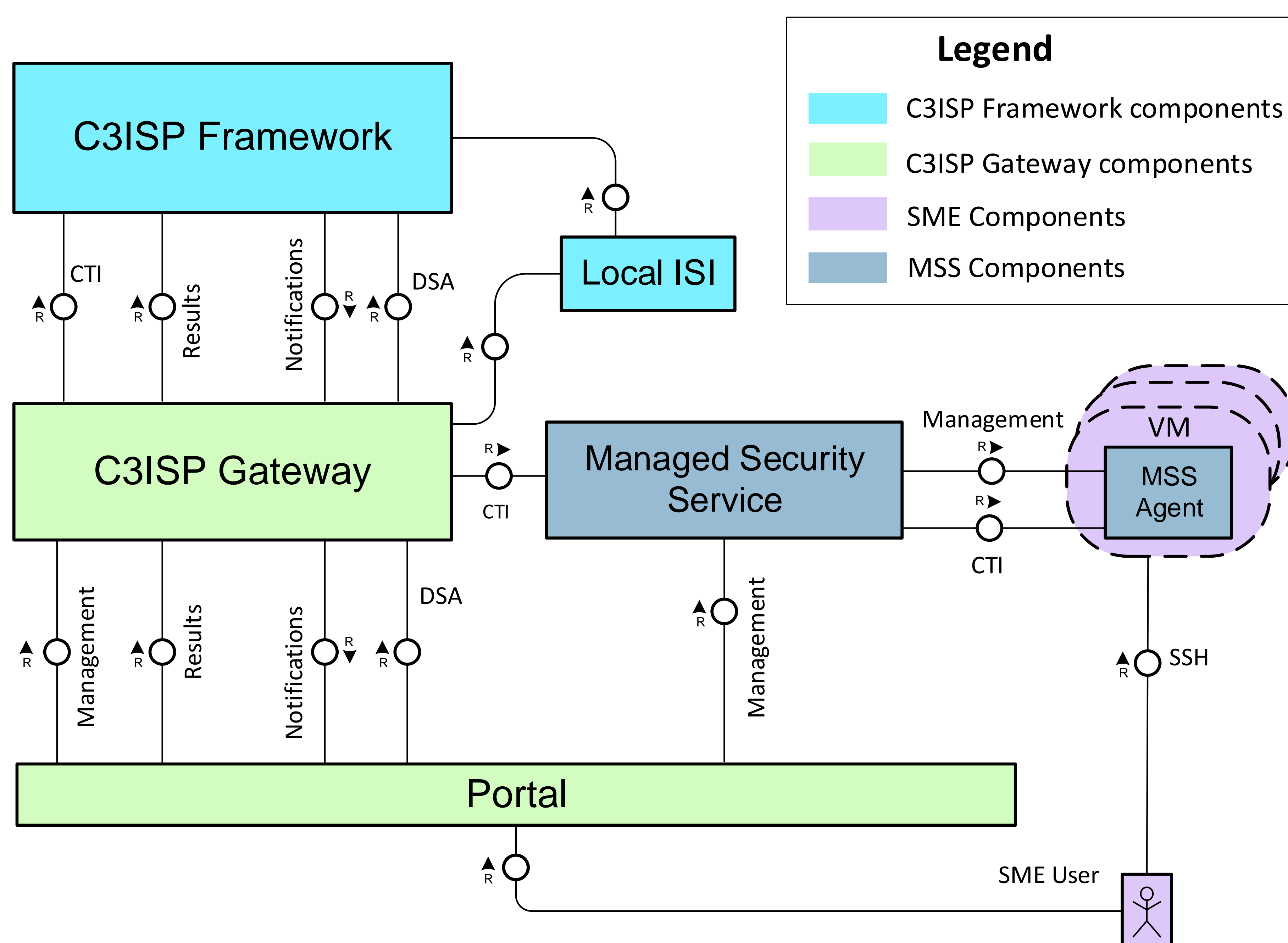


The C3ISP Framework enables organisations to share their Cyber Threat Information (CTI), in a privacy protecting way, for collaborative analysis in the cloud. It does this through the definition and enforcement of Data Sharing Agreements (DSAs).

The C3ISP Gateway is an organisation's interface to the C3ISP Framework. The Gateway retrieves CTI data from the organisation's Managed Security Service (MSS), combines it with a DSA, and uploads the encrypted object to the C3ISP Framework for subsequent sharing and analysis. Through an easy to use web interface (Portal) to the Gateway, the user is able to manage all of their C3ISP related tasks, i.e., choosing which CTI data to share, creating and selecting a DSA, and running collaborative analytics.



**Security:** Common security services (i.e. Identity Manager, Key and Encryption Manager, Secure Audit Manager) are available in order to satisfy the security requirements.

**Agreement:** The processing of CTI data is governed by the policies defined in a Data Sharing Agreement (DSA), which is a contract between collaborating organisations and the C3ISP Framework.

**Sharing:** Organisations share their CTI data under the constraints specified in a DSA's policies and C3ISP stores the CTI data ready for access by the analytics services.

**Analytics:** Organisations can request the execution of analytics services on the data protected and shared by the sharing service.

C3ISP's **benefits** allow organisations to:

- Have a global view of cyber threats
- Mitigate the security risks
- Avoid leaking sensitive information
- Reduce investment in solving security issues
- Increase customer confidence

