



*Secure single-window access to your web applications*

### Benefits

- Protects access to your critical applications with the security and reliability of SWIFTNet.
- Uses your SWIFTNet infrastructure as a single window access to multiple services. No need to set up and manage a new dedicated channel.
- Easy adoption of new services as your connectivity, infrastructure, tools and processes are already in place.

## SWIFT WebAccess

*Offering you secure and reliable access to your service provider's web applications over SWIFTNet*

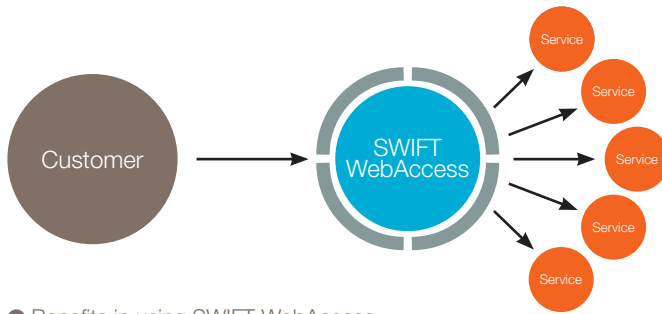
With regulatory requirements ever tightening, and security threats continually increasing, financial organisations now require a unique level of control over their operations. Critical financial operations need to be administered within a highly secure and controlled online environment in which users' access is strongly protected and actions are fully traceable to the individual user.

A variety of options exist for you to connect to these services, with internet or proprietary channels as common solutions. Yet, with cyber-threats an ever present risk, the internet may not measure up to the security and reliability demanded by mission-critical applications. On the other hand, proprietary channels require dedicated infrastructure set-up costs for each channel added, and require customers to use a variety of processes and tools, all of which may have implications on the resources needed to implement and maintain.

### Our solution

SWIFT WebAccess offers you a secure and reliable screen-based channel to access the interactive financial services offered by your providers over web portals – all by using your existing SWIFTNet infrastructure. By leveraging your current SWIFTNet infrastructure, you do not need to set up and manage dedicated connectivity (VPN), or other security mechanisms; and you further benefit from all the security and reliability of SWIFTNet. WebAccess also reduces user complexity by enabling you to access multiple applications using a single authentication method – enabling a simple, harmonised user experience.

SWIFT WebAccess builds upon our previous interactive service, Browse. WebAccess is distinct from Browse as it offers a SWIFT managed centralised authentication service (detailed above), offering you a single sign-on access to all your applications.



▲ Benefits in using SWIFT WebAccess

## Key features

- A secure and reliable channel to access your critical applications  
With WebAccess you can connect over the SWIFT-managed MV SIPN network, providing infrastructure resilience and multi-layered session-based integrity and confidentiality protection. Your users are strongly authenticated with individual SWIFTNet PKI certificates stored in hardware (HSMs or personal tokens), ensuring traceability of their actions individually. You control which users can access which applications.

### — Easy set up

You can leverage your SWIFTNet infrastructure to establish a new access to an application. No need to set up and manage dedicated connectivity (VPN), or other security mechanisms. Furthermore you have 3 options for using WebAccess: 1) over Alliance WebPlatform using certificates stored on HSM; 2) over a standard internet browser using certificates stored on personal tokens; and 3) over Alliance Lite2 using certificates stored on personal tokens.

- Single window across service providers  
WebAccess provides you with a single-window access to multiple services from different providers. You can re-use the connectivity, the infrastructure, the user environment and access methods, as well as the user management processes and tools across differing services. No need to set up and maintain new, individual channels for each application.

### — Single Sign On

You can use the same certificate to access multiple services over WebAccess. You login to WebAccess and obtain access to all your applications at once. WebAccess therefore provides users with

a harmonised experience in accessing applications from various providers as well as unique processes to manage user credentials and roles across differing services.

### — Non-repudiation service

Service providers can optionally request a non-repudiation confirmation over WebAccess for end-users to authorise critical transactions. WebAccess displays the transaction information sent by the service provider over a confirmation screen for review by the end-user. The end-user provides their confirmation by signing the transaction using their personal certificate, which ensures non-repudiation and traceability at the end-user level. SWIFT stores the signed transaction centrally for 124 days and can act as trusted third-party between the service provider and the end-customer.

## Costs

The costs include a monthly usage fee, which depends on the size of the service, as well as a per transaction fee if the service uses the secure transaction feature. The fees are included in SWIFT's Fixed Fee arrangements. Factors such as expected throughput may also impact on costs.

## Product features

- Channel security: MV-SIPN & HTTPS – Screen-based channel with the security and reliability of SWIFTNet, offering multi-layered encryption and integrity protection
- User-level security: SWIFTNet PKI – Strong user authentication based on SWIFTNet PKI certificates stored in hardware (HSM box or personal token)
- Single sign on: Centrally managed user access – User authentication is validated centrally, thereby offering users with single sign-on access to multiple services
- Access Control: Role-based access control (RBAC) – You control which of your users are authorized to access which application

## Optional features

- Transaction confirmation: Non-Repudiation service – SWIFT provides a complete non-repudiation service for critical transactions, enabling individual traceability of your operators' actions (with SWIFT as a trusted third-party)
- Flexibility of access: Internet support – your users can access applications over the internet if enabled by your service provider

For more information, please visit: the [SWIFT WebAccess webpage](#) or contact your SWIFT account manager