Formula Consultants

OTS-1100

Product Description

Formula Consultants Incorporated

P.O. Box 544
Anaheim, California 92815

714/778-0123
714/778-6364 (Fax)

sales@formula.com
www.formula.com

Highlights

OTS-1100 protects your OS 2200 online transactions from unauthorized use by validating user credentials in relation to transaction functions. You can establish a secure transaction environment without changing your online programs.

You can also use OTS in conjunction with DPS to implement field-level security. If you are able to modify your application programs, you can use the application interface (AI) in OTS to deliver authorization data to the executing program. That program can then make fine-grained decisions to permit or withhold individual transaction functions, based on the user's security profile.

Current Release	OTS-1100 6R7
History	OTS-1100 in production use since 1984.
Installation	Standard installation with SOLAR.
Comprehensive security for online access	Provides security for your online applications. Highly flexible installation and configuration options.
Plays with major Unisys features	TIP, DPS, MCB, CPComm/CPCommOS Application Groups.
Options without app changes	Several installation modes provide security for your online programs without changes to the application.
Field-level security	OTS integrates with capabilities in DPS.
Fine-grained permissions	Compile / LINK a program with OTS' application interface (AI). AI passes user/terminal profile properties to the application program The application program permits/denies functions based on data from AI.

Overview

Designed for Comprehensive Protection

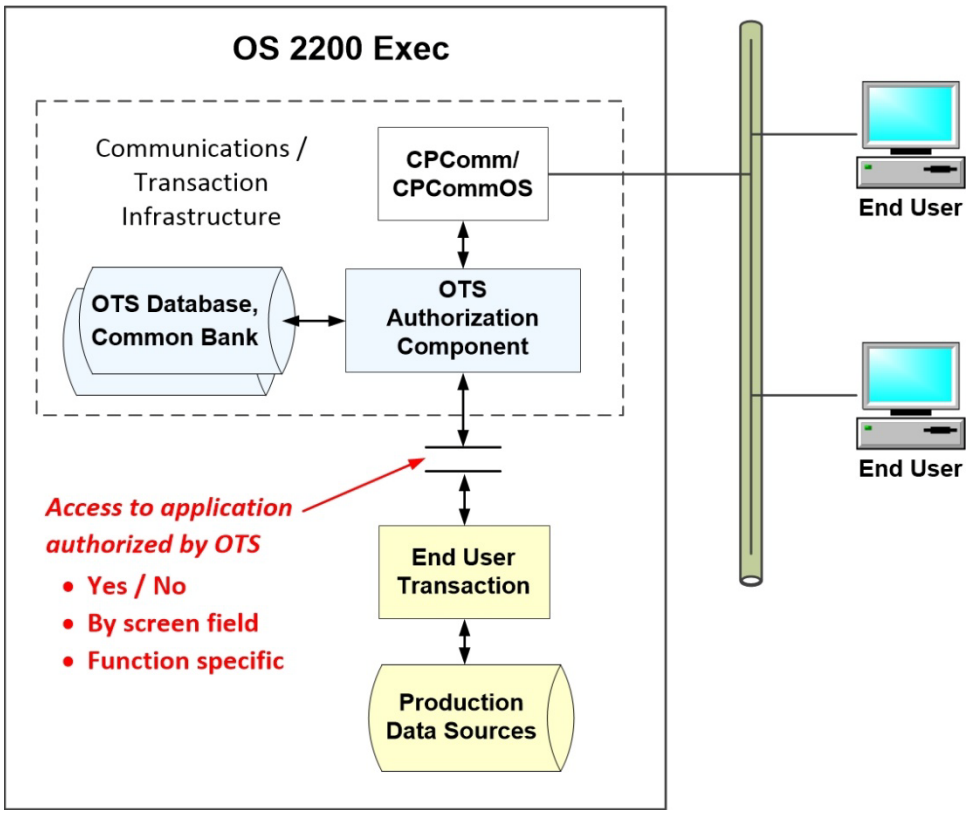
OTS-1100 is designed to give OS 2200 administrators a highly effective way to apply security authorization to all their online transaction programs, individually and within groups.

The Primary Purpose of OTS-1100

The primary purpose of OTS-1100 is to prevent unauthorized execution of transaction programs under OS 2200.

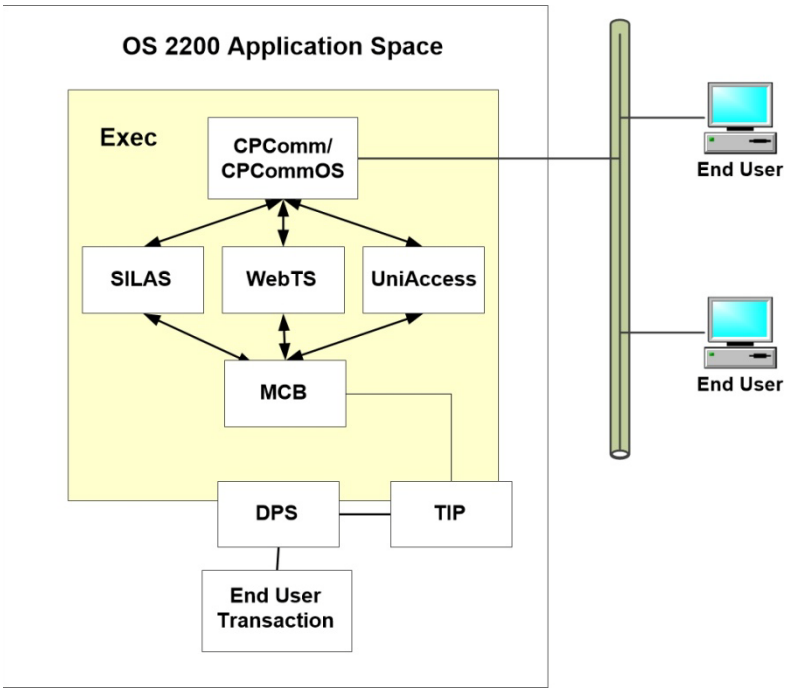
OTS implements a comprehensive security regime for your transaction environment, which provides high levels of protection. Users who are not authorized to execute certain programs are prevented from doing so. Or, they might be authorized to execute a certain program, but not all of its features.

OTS fulfills an important need in the OS 2200 enterprise for organizing access permissions broadly and specifically.



OTS-1100 Interoperates with EXEC Features

OTS-1100 is compatible with and interoperates with all the major OS 2200 EXEC features supporting transaction processing.



The diagram above shows the transaction flow between the user operating their terminal through to the application transaction program.

TIP and DPS are shown straddling the EXEC and the OS 2200 application environment. They both have core components within Exec internals, and user-accessible features.

See the next topic to learn how you can implement OTS-1100 to satisfy your needs for protecting your online transactions.

Options for Implementing OTS-1100

You choose installation options for OTS, based on your site's implementation philosophy for transaction systems and your goals for their security.

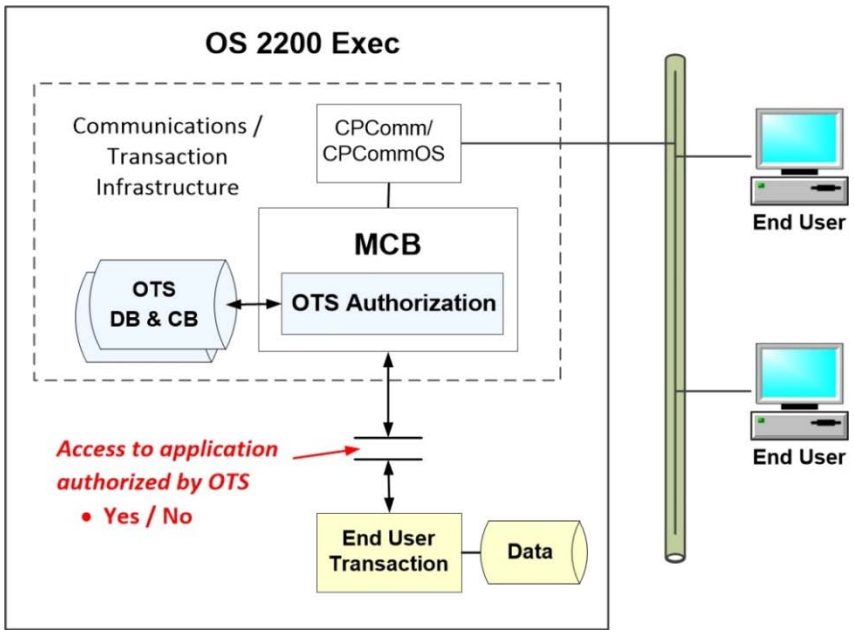
MCB Implementation

In this option, you BUILD the Unisys MCB product with an OTS-1100 component. When the user attempts to execute a transaction, MCB checks first with OTS to see if that user is authorized. If not, the request is declined.

This method of implementation is highly efficient because in an unauthorized request, the EXEC doesn't even load the transaction.

No changes are required to your transaction programs.

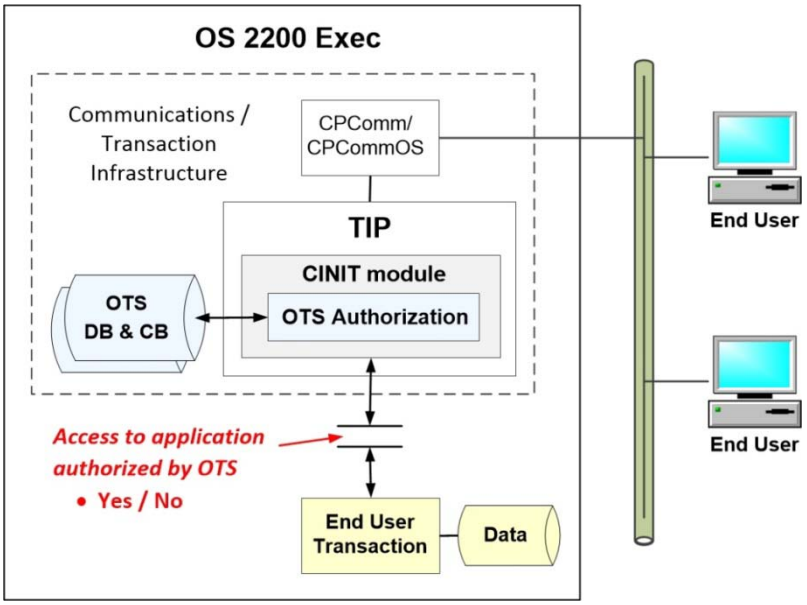
This approach is recommended for all MCB sites.



Authorization result:	Yes or No
Re-compile?	Not required
Re-link?	Not required

TIP Implementation

In this option, you BUILD the Unisys TIPUTIL product with OTS code inserted in the INITAL module. When the user attempts to execute a TIP transaction, the transaction's call to CINIT in the INITAL module checks first with OTS to see if that user is authorized. If not, the request is declined.



Authorization result:	Yes or No
Re-compile?	Not required
Re-Map?	REQUIRED Re-map your transaction with INITAL

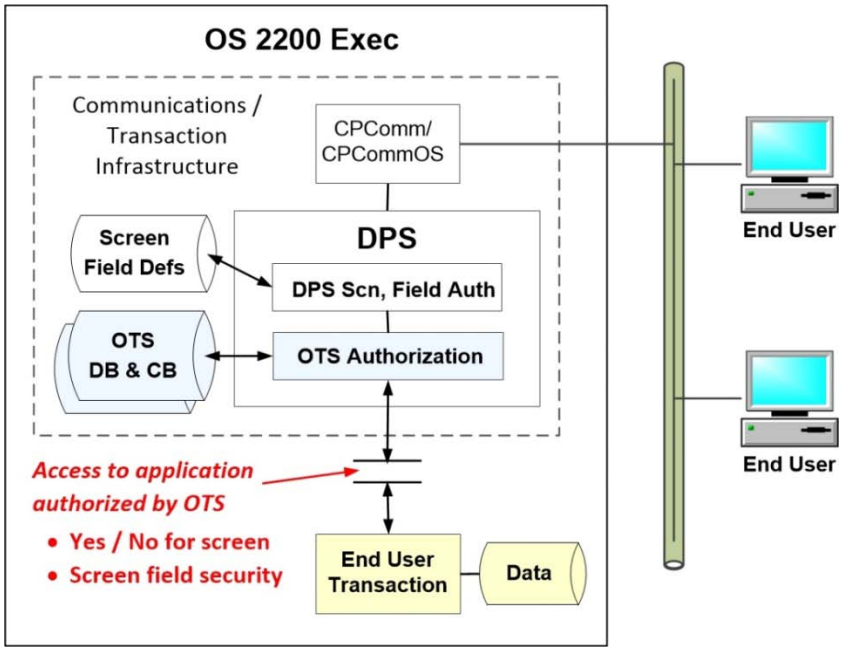
DPS Implementation

In this approach, you have several ways to protect transactions and their data. You can permit or reject the transaction and presentation of a screen associated with the transaction. And, you can pre-define the security values for each field presented on the DPS screen.

In this option, you BUILD the Unisys DPS product with OTS code inserted in the modules ACOB/INTERFACE or UCS/INTERFACE.

You re-map or re-link your transaction with the ACOB/INTERFACE or UCS/INTERFACE modules of DPS. When the transaction calls D$INIT, the interface checks first with OTS to see if that user is authorized. If not, the request is declined. Then if the if the screen itself is not authorized, the user cannot execute the transaction. If you have defined field-level security, DPS checks the credentials of the user and presents only those fields with security values equally or less stringent than the values associated with the user.

With OTS, a user can have a different DPS Screen security level for each OTS transaction group and a different DPS field security level for each transaction within that transaction group.



Authorization result:	Yes or No for the screen, Authorization for individual screen fields
Re-compile?	Not required
Re-map/Re-link?	REQUIRED Re-Map/Re-link your transaction with the ACOB/INTERFACE or UCS/INTERFACE modules (DPS)

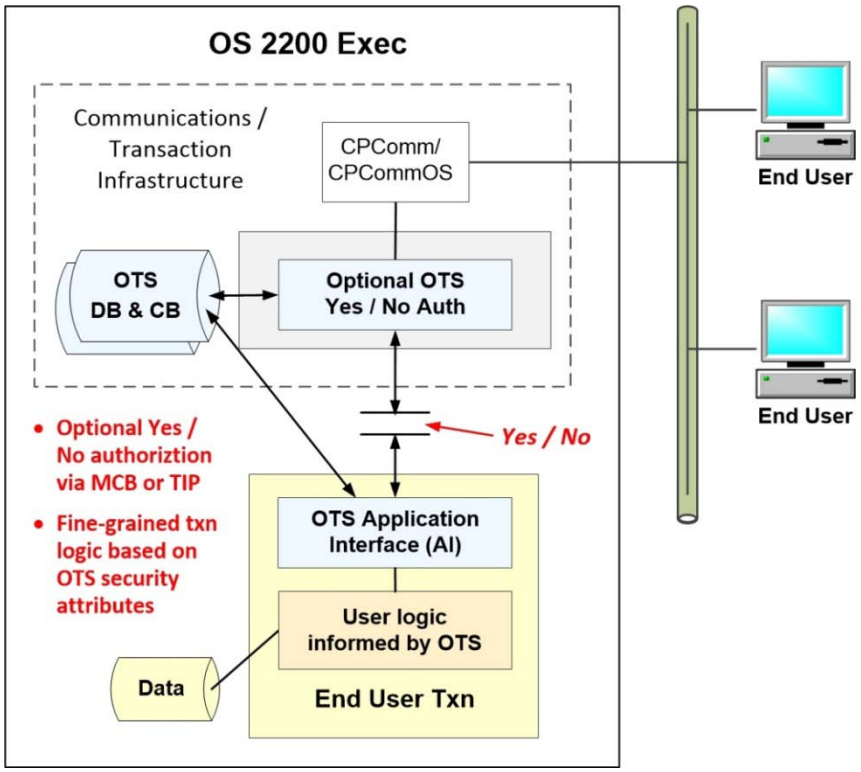
Application Interface (AI) Implementation

In this approach, you have re-compiled and re-linked your transaction to include the OTS Application Interface module (AI).

The programmer calls OTS directly, through the application interface, and receives the security profile of the user. The programmer then codes decision logic to differentially read and/or write data, and present information on the screen, based on the security profile of that user.

This permits you to implement very fine-grained authorization.

If you want to also achieve a Yes / No authorization, you can also implement the MCB method (see the next topic).



Authorization result:	Unique results in each transaction, based on the coding of security checking in relation to the user values passed by OTS Note: Yes / No authorization is available by also implementing the MCP or TIP approach
Re-compile?	REQUIRED Re-compile the transaction with the OTS AI module
Re-Map/Re-link?	REQUIRED Re-Map/Re-link your transaction

Combining Authorization Methods

OTS-1100 Security Administrator's Guide

To achieve your goals in managing and protecting your online transaction environment, you might implement more than one authorization method. As you review the OTS product documentation, you will learn about the best ways to take advantage of the flexible implementation options.

For example, you could use the MCB implementation to make certain you have strong authorization for whether or not a user can execute a transaction. You could also implement DPS field-level security for a set of your transactions.

OTS-1100 Programmer's Reference Guide

Perhaps you have a program with a history of critical legacy use by a large user population with widely ranging security profiles. For transactions like this, you can compile and link the OTS Application Interface (AI) into the program. Early in the execution process, the program can call AI to receive the security profile of the user. The program can then permit users to operate only those features and actions which match their authorization levels.

Additional Features of OTS-1100

User Oriented Features

System Sign On Options

OTS implements a unique transaction, SIGNON, for all users logging onto the transaction environment. This ensures that users are operating under the protection of OTS-1100. TIP and DPS also have sign on regimes. Your system administrator has several options for integrating OTS with the other existing methods of user authorization in your transaction infrastructure.

TIP Session Control is a feature of the EXEC related to Application Groups defined within the Integrated Recovery feature of OS 2200. TIP Session Control gives administrators additional options for logging into the transaction environment. OTS-1100 is well integrated into the options for configuring and using TIP Session Control.

Monitoring Security Violations

When a user attempts to execute a transaction for which they are not authorized, they receive a rejection message on their workstation. OTS also increments a count of violations in their user record. When a user exceeds a pre-configured maximum number of violations, their access to the transaction environment it suspended. They can be re-activated only through intervention by a highly privileged administrator.

Password Expiration

Administrators set the expiration period for users' passwords. Users change their passwords more frequently, improving security.

Designated Initial Transaction

Some users follow a work-flow pattern where they select a specific transaction first, each time they sign on. System administrators can designate an initial transaction for the user. When the user signs on via OTS, this designated transaction will be scheduled first, automatically.

Infrastructure Features

Hierarchical Administrator Privileges

OTS establishes administration capabilities at several levels of privilege. The most privileged administrator can delegate tasks to sub-administrators, who are privileged to perform more routine maintenance tasks within OTS.

Transaction Groups

You can organize your transaction programs into groups. You configure OTS to permit certain users to have access to only the transaction groups which you specify. This simplifies the configuration process for administrators.

For example, accounting staff can be authorized for only an accounting group of transactions. Or, administrators can differentiate more narrowly, assigning lower level accounting staff to a transaction group with routine, data entry or reporting transactions. Accounting staff with greater responsibility can be authorized for a transaction group with accounting programs of greater consequence and with higher privileges.

The field-level security techniques available through DPS are managed through OTS transaction groups.

UniAccess

OTS-1100 supports UniAccess transactions within its overall transaction management and protection.

Global Transactions

You may have a set of transactions which pose no security risk. When you define these to OTS as global transactions, OTS bypasses logon authorization requirements. This is analogous to the open, public pages of your organization's website. You permit, even encourage, access by all users.

Even when a transaction is designated as "global," you have the flexibility to configure access to suit your specific needs.

Management

Reporting

OTS-1100 provides reports for:

- security records for users and programs,
- user activity,
- exceptions, including authorization violations

Development and Testing

OTS-1100 offers several ways you can confidently test new or modified transaction programs before promoting them to production status.

There are convenient and simple commands to enable and disable transaction groups.

OTS-1100 Components

OTS-1100 has components for installation, configuration and operation.

- **A Security Database,** implemented under DMS-1100, contains the security profile of each user and information about programs and terminals.
- **A Security Common bank**, holds code for frequently executed modules and tables for efficient security checking.
- Modules to implement **authorization**. OTS modules are installed in OS 2200 features such as MCP, TIP, and DPS, to fulfill OTS' primary purpose of authorizing user access. See the diagrams and explanation in the topic "Options for Implementing OTS-1100."
- **Application interface (AI)** to implement fine-grained differential security. Programmers call OTS directly to interrogate user credentials and make decisions about subsequent processing.
- Online **session control** components. Basic transactions for users to log onto the transaction system and log off. These replace the standard "signon" and "signoff" transactions.
- **Utility programs** for initializing and maintaining the Security Database and the Security Common bank.
- **Documentation** to assist administrators in installing, configuring and operating OTS-1100.

OTS-1100 System Support Manual

Product Documentation

- *OTS-1100 Online Terminal System 6R7 Release Announcement*
- *OTS-1100 System Support Manual*, FP-123 R9
- *OTS-1100 Security Administrator's Guide*, FP-119 R9
- *OTS-1100 Programmer's Reference Guide*, FP-124 R9
- *OTS-1100 User's Guide*, FP-122 R9