LiveEngage Secure Form

Document Version: 1.2
June 2018

LIVEPERSON

Contents

Introduction

LivePerson invests heavily in providing the most secure platform possible for our services, customers, and their data. As veterans in the field, we understand that security is especially paramount in correspondence between agents and consumers and requires a heightened level of protection. The LiveEngage Secure Form was specifically designed to provide the additional security layer that enables consumers to be able to, in full confidence, provide their sensitive information (such as Cardholder Data /CHD, social security number, and other Personal Identifiable Information/PII) in a highly secure environment.

Secure Forms are supported both on desktop and mobile web.

Secure Form Benefits

The LiveEngage Secure Form provides brands with an enhanced engagement experience with the following benefits:

- **Extra Secure Interaction**: The Secure Form dedicates a "secure tunnel" within the standard chat for exchanging Personal Identifiable Information (PII), Cardholder Data (CHD), and other sensitive identity validation data like answers to verification questions and PINs. Agents continue to operate in the same Agent Workspace environment as data is sent from the visitor to the agent in a safe, PCI compliant interaction.
- **No Storage of Sensitive Data in Chat Transcripts**: Data processed by the Secure Form is not stored as part of the standard chat transcripts and cannot be retrieved through the application after the chat session has ended. The data is securely stored in its tokenized form in a dedicated database.
- **Off the Record Questions (CVV):** The LiveEngage Secure Form offers the option of "Off the Record" or CVV verification questions. In both cases, the visitor's answers are not stored anywhere (not even in tokenized form), and are only available to the agent in real time. This question type can be used for asking the visitor CVV information in a secure PCI compliant manner.

European Security Standards

LivePerson works hard to ensure that our customers around the world can safely and securely use our platform. There are several different standards for protecting data around the world. LivePerson meets the following international standards for data protection, ensuring that our European customers can safely use our Secure Forms:

1. **Standard 1: PCI-DSS**
    a. LivePerson complies with Payment Card Industry Data Security Standards (PCI DSS) 3.2 for it's Secure Form Widget and Billing system. To view the certificate, click here.
2. **Standard 2: GDPR**
    a. LivePerson has worked to ensure compliance with the EU General Data Protection Regulation (GDPR). Please read more on the LivePerson website.
3. **Standard 3: US: Privacy Shield certification**

a. LivePerson has had European operations for years is compliant with the current European data privacy rules. To learn more, click here.

When to Use the LiveEngage Secure Form

Some of the most common use cases for the Secure Form include:

- Visitors need to provide their credit card information to an agent.
- Visitors need to provide their CVV number to an agent.
- Visitors need to provide PII to an agent as part of the identity validation process, for example, to answer a secret question.
- Any other situation requiring the visitor to send sensitive information to the agent.

PCI-DSS Compliance

The LiveEngage Secure Form is specifically designed to comply with the strict requirements of the Payment Card Industry Data Security Standards (PCI-DSS). The form was developed under the guidance of a Qualified Security Assessor (QSA) and a dedicated PCI-DSS environment hosts the Secure Form system components.

Following the completion of an onsite assessment, the LiveEngage Secure Form environment has been officially certified as compliant with the requirements of a Level 1 Service Provider PCI-DSS (version 3.1). Attestation of Compliance (AOC) can be provided upon request.

How it Works

An agent can send a Secure Form from the Agent Workspace at any time during a chat session by clicking the Secure Form tab in the Predefined Content widget and selecting a Secure Form.

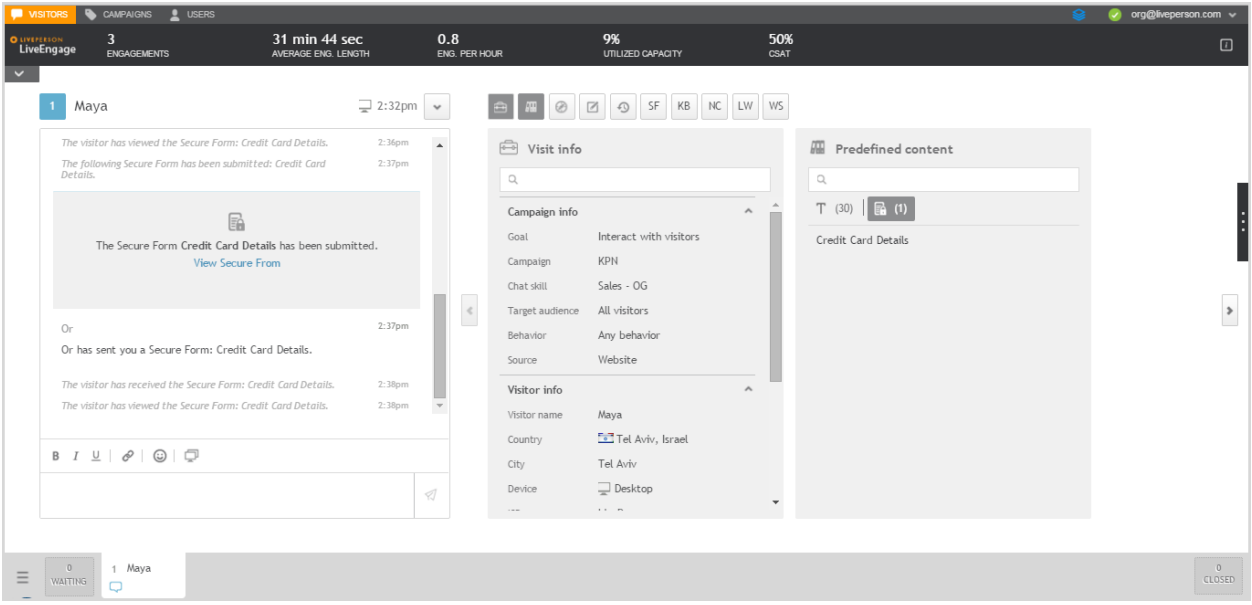

Figure 1: Secure Form within the Agent Workspace

The visitor then fills out and submits the Secure Form back to the agent. The receiving agent is the only one able to view the information sent by the visitor.

Note: If there are other agents viewing the chat, they will not be able to view the Secure Form. In addition, agents who receive a transferred or reassigned chat will not be able to view the Secure Form. Only the agent who sent the form can access the submitted form.

Example of a Secure Form in use:

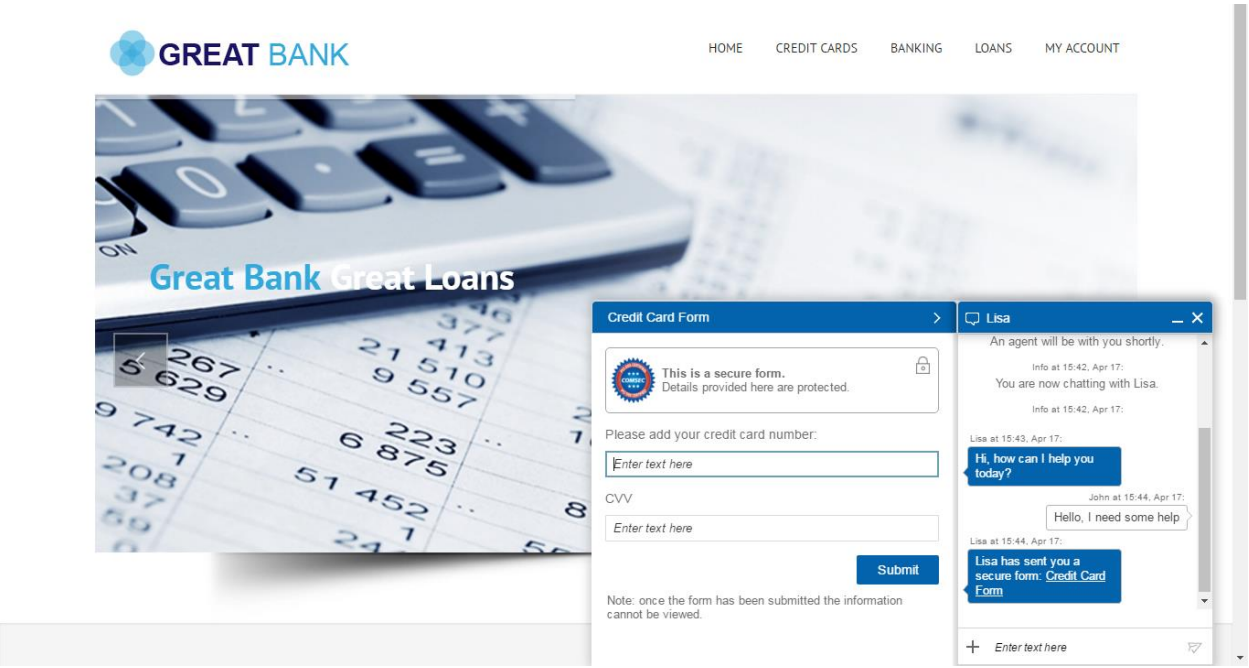

Figure 2: LiveEngage Secure Form within an Engagement Window Interaction

Fully Accessible Visitor Experience

The Secure Form widget complies with ADA and WCAG 2.0 AA disability accessibility requirements. This applies to both the desktop and mobile web (iOS and Android) and includes:

- Screen reader support: Secure Forms can be filled out using screen readers for visually impaired visitors.

- Keyboard operable: Secure Forms can be operated without the use of a mouse for visitors with motor function and/or visual impairments.
- Improved error handling: Clear error indication and suggested fixes.

Data Flow

Tokenization is a method of substituting data to render it meaningless to anyone gaining unauthorized access. The tokenization processes implemented in the Secure Form environment is based on a technology manufactured by a leading provider of tokenization solutions. The sensitive data submitted in the Secure Form is sent from the visitor to the agent via the PCI-DSS certified environment. A dedicated PCI compliant server handles the tokenization of the sensitive information and validates agent authorization before delivering the visitor-submitted Secure Form.

The following diagram shows the process and security layers of a visitor completing a Secure Form and sending it to an agent.

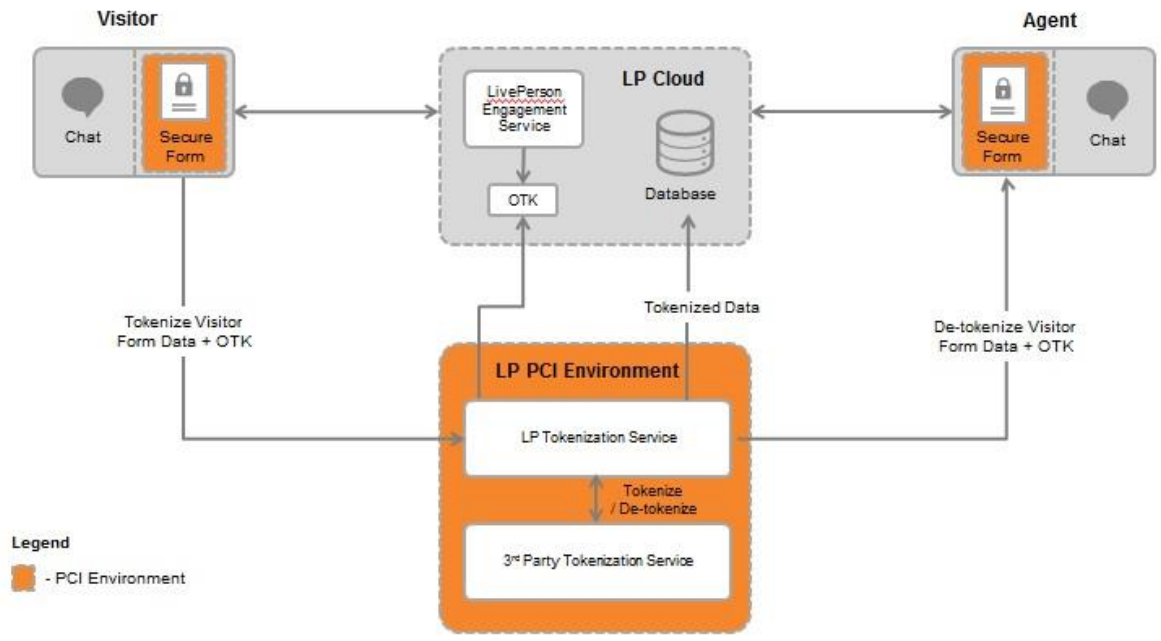

Figure 4: Secure Form Visitor to Agent Flow Chart

Below is a detailed explanation of the flow of the diagram above:

4. The agent sends a Secure Form with a one-time token (OTK) for retrieval.
5. The visitor receives the Secure Form using the OTK and submits it using a different OTK.
6. The data is tokenized. The tokenized data is not legible by anyone outside the service, and moreover, the token is assigned to a specific action in the environment. For example, you cannot use a submit data OTK to retrieve data.
7. The data is stored in its tokenized form in a dedicated database and is represented by a Universally Unique Identifier (UUID). This means that the tokenized data is never directly accessible to any client outside of the LivePerson environment. Rather, the client receives the UUID and requests the data from the PCI environment. "Off the Record" data (CVV) is not

stored in the database, but is stored in memory for a short period of time. After this time period, the agent will need to resend the form in order to access this information.

8. The UUID along with another OTK is sent to the agent.
9. The agent retrieves the form via the OTK and UUID.
10. The service detokenizes the data and sends it back to the agent.

Security Measures

The Secure Form solution was designed with strict security parameters to help ensure sensitive customer information is sent only to the appropriate, authorized agent (these controls are in addition to the standard controls required by PCI-DSS). The following controls have been implemented as part of the solution:

- Data sent from the visitor by means of the Secure Form undergoes a tokenization process.
- Access to the tokenized data requires authentication and session validation.
- A unique one-time key (OTK) is utilized for each form initiated by an agent. Each OTK can only be used once and is valid for a very short period of time (seconds).
- One-time-keys undergo validation and verification during the data de-tokenization process.
- The visitor's OTK can only be used for tokenizing the data. The agent's OTK can only be used for detokenizing the data. Moreover, an OTK is specific to one site. This ensures that the OTK cannot be inappropriately manipulated.
- The sensitive data is only accessible during the active session. It is not stored in the chat history or transcripts.
- The tokenized data is securely stored in the LivePerson application database in its tokenized form for a default period of 13 months. Currently, the application does not provide access to retrieve the tokenized data.

Supported Browsers

Refer to System Requirements for information about supported browsers.

Considerations when Using Secure Forms

When using Secure Forms, bear in mind:

- Submitting CVV (Card Verification Value) or CVC (Code Verification Certificate) data should only be performed in CVV question type or questions that are marked as "Off the Record".
- Data submitted in the Secure Form is only retrievable for the duration of the session it was submitted in.
- Agent workstations utilized for viewing Secure Forms are in-scope of PCI-DSS certification.
- LivePerson Accounts Password and Login Policy must be enabled and configured according to PCI-DSS requirements.

Setting up LiveEngage secure forms

Secure forms are configured by LivePerson. To enable this feature, please contact LivePerson Customer Support or your account team. Your LivePerson account team will work with you make the necessary adjustments to your account settings and configurations.

Account setup

Once secure form features have been enabled on your account, your LPA will need to setup your account for secure forms. The following parameters will need to be configured in order for secure forms to work on your account; if you require different account settings, please discuss this with your LivePerson account team.

The **Account Password Policy** will be configured as follows:

Setting	Required Configuration
Minimum number of characters	Set to minimum 7
Alpha character required	Required
Number character required	Required
Apply policy to current passwords	Required
Expires after number of days	Set to 90
Prevent using previous number passwords	Set to minimum 4

The **Failed Login Policy** will be configured as follows:

Setting	Required Configuration
Automatically disable operator after number of failed logins	Set to minimum 3
Number of minutes before re-enabling disabled operator	Set to blank

The **Idle Operator Policy** will be configured as follows:

Setting	Required Configuration
Automatic action when operator is logged in but idle	Set to: “Logout the operator”
Logout operator from the account after minutes of inactivity	Set to maximum 15

Permission settings

The following permissions related to secure forms need to be enabled for an account:

Role	Permission	Permission definition	Default State (role)
Agent	Use secure form within a conversation	For brands who have enabled the secure forms feature, this permission allows the Agent to use the form within a conversation	**On**

Note: The following permission for Agent Managers also relates to secure forms, but does not need to be enabled unless you wish Agent Managers to be able to view secure form responses in the Engagement History.

Role	Permission	Permission definition	Default State (role)
Agent Manager	View secure form responses in Engagement History	For brands who have enabled the secure forms feature, this permission allows the Agent Manager to view all secure form responses in the Engagement History	Off

To verify that permissions are enabled:

1. In the Users tab, click on the Profiles page.
2. Click on the 'Agent' profile. The Edit profile page will open.
3. Under Permissions, scroll down to confirm that the 'Use secure form within a conversation' permission is enabled.
4. Click Save.

Note: If a you would like to enable the secure forms permission for some agents, but not for others, this can be achieved by creating a new custom profile within the agent role. For further information, refer to the Customize user profiles documentation.

LivePerson Technical Support

LivePerson Technical Support is available 24/7 in the LiveEngage Connection Area.